CONTROLLER 3000 SERIES

WIRELESS CONTROLLER 3000

NETWORK CONTROLLER 3000

NETWORK CONTROLLER 3500

USER MANUAL

ABOUT THE MANUAL

Please read this manual before working with the Controller 3000 Series (Wireless Controller 3000 or Network Controller 3000/3500). This manual is intended to provide a basic understanding of the Controller 3000.

Although utmost care has been taken to provide all the information in this manual that is required to understand the functionality of the Controller, any additional inquiries can be mailed to: support@valuepointnet.com.

USAGE AND FEATURES OF THE MANUAL

To make it easy, this manual has a simple structure and the user can easily navigate through the sections to understand the various features of the Controller 3000. The first section introduces the user to the Controller 3000, its package contents, features and precautions to be taken while using the Controller.

The second section describes the Installation Requirements and steps. Follow them carefully for successful installation of the Controller 3000.

The third section describes the Configuration details of the Controller 3000.

CONTENTS

1. INTRODUCTION

This section of the Manual gives an overview of the Controller 3000 along with the Package Contents, Features and Precautions.

Overview

The Controller 3000 was developed with an aim to provide high-speed access to the Internet for Public Networks. The Controller 3000 is deployed in a wireless broadband service network, which can recognize new users on the network and redirect them to the appropriate connection. In short, the user can access the Internet without changing configuration settings or needing technical assistance no matter what their configuration.

Package Contents

The package contents of the Controller 3000 are:

1. One Controller 3000/3500
2. One AC Power Adapter
3. One CD containing user's manual & Quick Start Guide
4. One UTP Ethernet/Fast Ethernet cable (Cat.5 Twisted-pair)
5. Two removable 4dbi omni-directional antennas

Features

Some key features of the Controller 3000 are:

☞ **Advanced Local Authentication**

Authentication can be controlled totally within the Controller 3000 using a local user database of 512 username/password accounts. Unlike the typical primitive Local Authentication feature on most HotSpot Gateways, Controller 3000 local accounts are richly manageable by account start and end dates and access time.

☞ **Auto-IP Support of Subscriber IP Settings**

The wireless subscriber can access the Controller with no change to his existing IP related settings, such as IP address, subnet mask, or default gateway IP address in his notebook computer. No matter what settings the subscriber has in the notebook computer, the subscriber always can access the Controller.

Note: The 'Auto-IP' Function can only be used with TCP/IP-based Networks.

☞ **HTTP Auto-Proxy Support of Subscriber Browser Settings**

Some subscribers will have a HTTP Proxy configured in their web browser, generally as part of their corporate configuration. The Controller will automatically detect and re-route these proxied HTTP requests to provide seamless connectivity to the subscriber.

☞ **Bandwidth limiting to insure Quality of Service for all subscribers (3500 only)**

Bandwidth usage by any single subscriber can be throttled back to the configured bits-per-second (bps). This prevents any one user from monopolizing the network.

☞ **Secure Management via XML and SOAP**

XML combined with SOAP allows rich, full featured, and secure control and monitoring of the Controller 3000. The Controller 3000 SOAP interface works today with Hampton Inn's HSIA Authentication, with future releases supporting Airpath Wireless' WIBOSS™ Control Center and more.

☞ **SMTP REDIRECTION**

Corporate and ISP mail servers often will not accept E-Mail from another network. With the Controller 3000, subscriber's outgoing SMTP server requests can be redirected to a SMTP server specified by administrator, so the subscriber can send out their email without changing the E-Mail configuration in their notebook computer.

☞ **Café Account™**

Customers can be given free access to the Network for a defined period, after which they would have to purchase more time to continue to browse or access the network from their laptop. This is ideal to allow free "use but don't abuse" access to draw customers into the venue.

☞ **Remote Configuration**

The Controller 3000 is easy for administrators to manage through the Web-based interface. The Web-based management is client-independent and is done by securely authenticating the administrator over SSL.

☞ **Custom Branding of Subscriber Experience**

The venue owner or system integrator can customize the branding and messaging for each HotSpot. Login pages, messages, and advertising can all be configured to match the Café, Hotel, or Airport experience.

☞ **"Captured Portal" Home Page Redirection**

The Controller 3000 allows the venue owner to redirect subscribers to a corporate web site or custom portal, where branding, login methodology, billing, terms of service, and more can be controlled.

☞ **Authenticated User Pass-through**

After their initial login to validate their account, subscribers can be given access to the network without needing to Login each time to their account. This means fewer lost and forgotten passwords and account names.

☞ **Walled Garden**

A walled garden provides pages or web sites that can be accessed by subscribers without requiring authentication. The Controller allows up to 266 destination IP addresses and URLs.

☞ **VPN (Virtual Private Network) Pass-through**

The Controller 3000 allows subscribers to access their existing VPN network at home or at the office. Unlike most public access gateways, the Controller allows all VPN connections through NAT and multiple connections to the same VPN server from a single venue.

☞ **Login Pass-through by IP or MAC Address**

The Controller 3000 allows a list of client computers to access the Internet without requiring authentication. The Controller allows up to 512 registered MAC addresses.

☞ **Secure HTML Login Page (SSL)**

Login Page utilizes SSL to protect username and password during User login.

☞ **Hardware Heartbeat Monitor**

This feature enables the Controller to continue functioning by resetting the system if the device experiences any problems due to unusual network activity (e.g. subscriber worms, viruses, or Denial of Service Attacks).

☞ **Sophisticated Syslog Monitoring**

A sophisticated System Log (Syslog) server is built-in to log events and enable automated monitoring. The System logs can be stored internally or events can be broadcast to a local or remote Syslog Client.

☞ **RADIUS Authentication**

Subscriber authentication on the Controller 3000 can be configured for the industry standard RADIUS AAA. RADIUS allows you to control multiple sites from a single NOC, or purchase authentication services from a third party billing provider.

☞ **Subscriber VLAN**

Subscribers and local network machines can be isolated from one another using Subscriber VLAN. This prevents users from accessing or molesting each other on the public network, or accessing enterprise hardware belonging to the venue.

☞ **Time based authentication list upload**

Security and Pass-through information for the entire enterprise can be centralized and updated in each controller automatically on a schedule. This allows for easy synchronization of both authenticated and "blacklisted" user information between multiple venues.

☞ **Terms of Service Based Authentication**

The Controller can be configured to enforce agreement to a customizable and branded terms of service page before subscribers can access the service.

- **Public Static IP Pass-through**

  Multiple Public Static IP addresses can be provisioned and distributed automatically to subscribers. While preserving the authentication, security, and branding features of the venue, these subscribers will have full access to their public IP for more sophisticated applications like VPN.

Precautions

Please carefully read the following precautions before using the Controller 3000:

- Do not remove or open the enclosure. You could damage the Controller or suffer injury if you tamper with the Controller hardware.
- The Controller 3000 enclosure is not water resistant. Avoid deploying the Controller where it might get wet.
- Only connect the supplied AC power adapter, or an adapter of the exact same configuration and power characteristics. Using the wrong adapter could cause damage to the Controller or a dangerous electrical shock to the user.
- The Controller 3000 enclosure is not heat resistant. Do not deploy the Controller 3000 in direct sunlight or in proximity to another heat source.
- Please deploy the Controller 3000 where it is well ventilated.

2. INSTALLATION

This section of the Manual gives information regarding the requirements and installation procedures for a successful installation of the Controller 3000.

Requirements

Check the following requirements installing the Controller 3000.

1. SYSTEM REQUIREMENTS

System requirements:

Management System:	PC with Ethernet or Wireless 802.11b network card
ISP Connection:	xDSL modem, Cable modem, or T1 Router.
Management Software:	Web Browser (Internet Explorer 6.0+ or Safari 2.01+ only)
Others:	Network Cable with a RJ-45 connector

2. WAN NETWORK REQUIREMENTS

Find out from your ISP whether the Controller will use a static or dynamic IP address. The most common configuration is DHCP, which assigns the IP addresses dynamically. If you are using a static IP address, you will need to get the full configuration from your ISP.

Dynamic IP	Set Controller to DHCP Client
Static IP	Controller IP address Controller subnet mask Default gateway IP address Primary/Secondary DNS Server IP addresses
PPPoE	User name from your ISP Password from your ISP

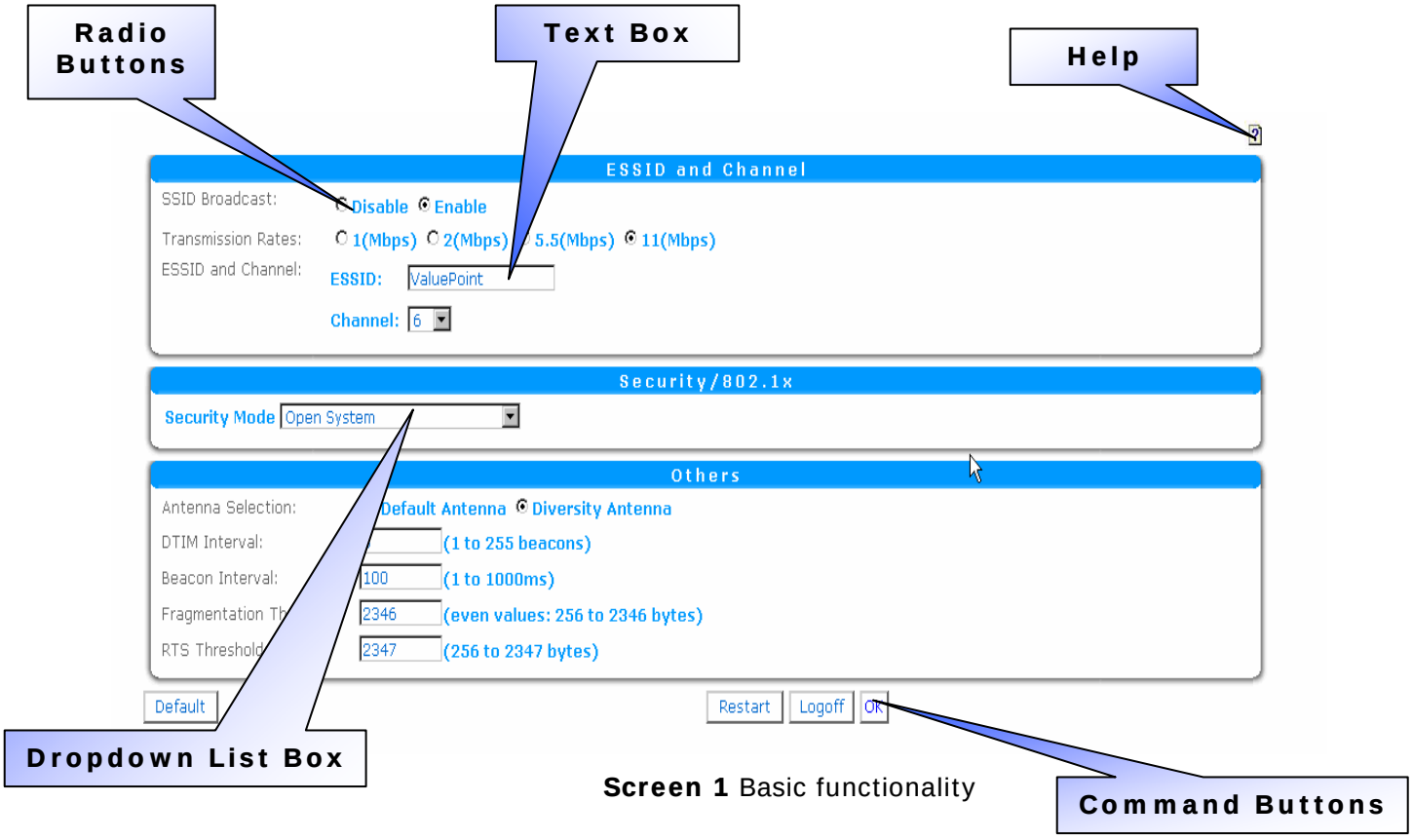
Note:
1. The Controller's default LAN IP address setting is '192.168.1.1'.
2. The Controller's default LAN subnet mask setting is '255.255.255.0'.

3. CONFIGURATION

This section of the Manual will give you information regarding access, login and usage of all the features of the Controller 3000.

3.1. BASIC FUNCTIONS

The screen below shows the type of options the user will come across frequently while configuring the system. Description about the use of each part is available in next section along with the instructions on its usage.



Screen 1 Basic functionality

1. CHANGING GUI SETTINGS

ENTERING DATA IN A TEXT BOX

To enter a data value in a text box click inside the text box and start typing. If the text box already contains some value, click at the end of the written text value and delete it with the backspace key. If the text box is grayed-out, this means the text is not editable.

SELECTING A VALUE FROM DROPDOWN LIST BOX

To select a value from a list first click on the arrow that is found on the right side of this list box and then select a value desired from the displayed list.

RADIO BUTTONS

To select a radio button simply click on the desired radio button.

COMMAND BUTTONS

To perform the actions as captioned on the button simply click on the button. For example: In the screen above, to apply the changes, simply click **Apply** to implement the changes made.

HELP

To view the help for some menus, click on the Help icon displayed on the right top pane of the menu.

2. RESETTING TO FACTORY DEFAULTS

SOFT RESET

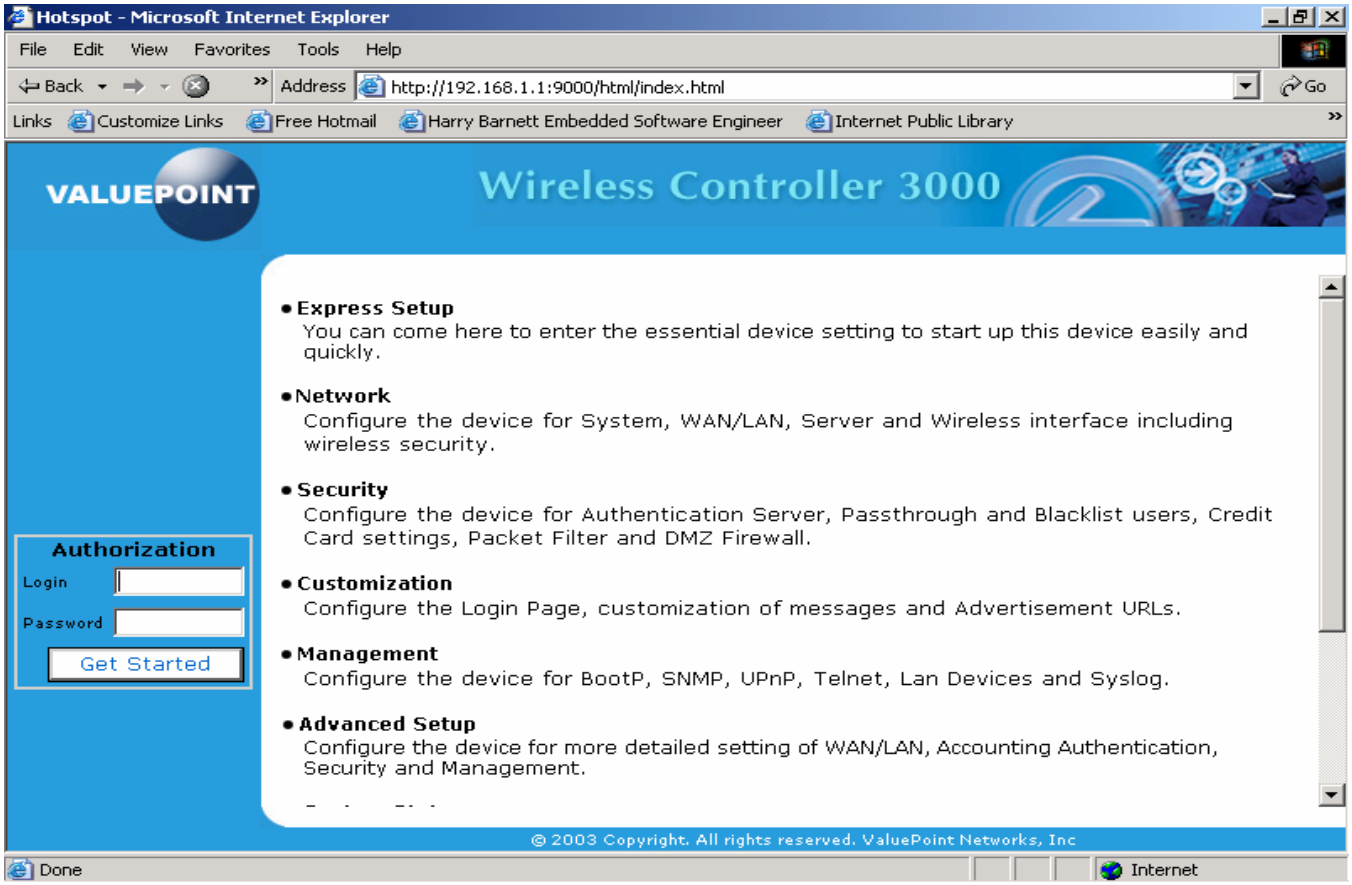
Connect to the Controller WEB GUI and navigate to **System Tools – Factory Settings** and select **Reset Factory Defaults**.

HARD RESET

Once the unit has booted and the “System” light is flashing or solid, press the button labeled “Default” on the face of the Wireless Controller for ten seconds and release. The Controller 3500 only has one “Reset” button, so hold that button for fifteen seconds to reset the 3500. When the system light goes out this means that the Controller is rebooting. After rebooting, the Controller will be accessible at the default LAN IP Address of **192.168.1.1**.

3.2. USING THE WEB MANAGEMENT INTERFACE

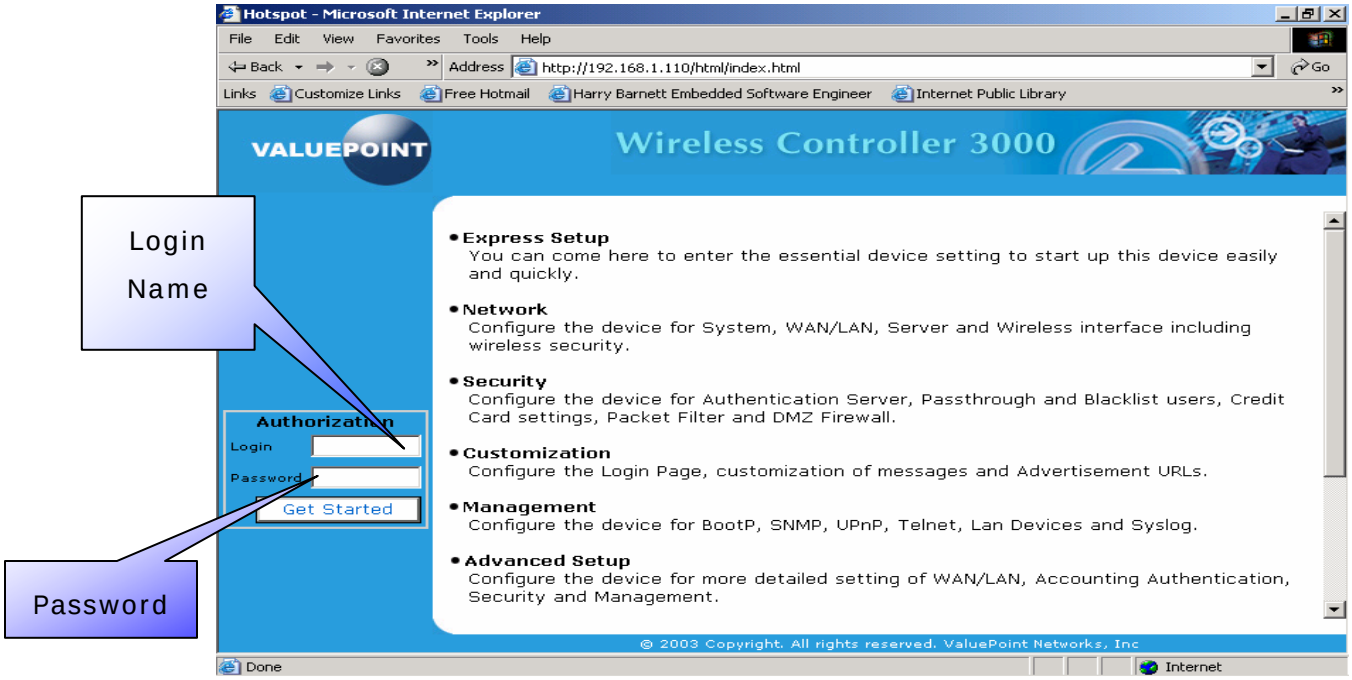
To access the Controller 3000 and utilize its menus enter the WAN or LAN IP address in the browser and press 'Enter'.



Screen 2 Controller Welcome Screen

3.2.1. LOGGING INTO THE CONTROLLER 3000

On performing the above steps, the Controller 3000 Home Page will appear on the screen as shown below. Through this Home page, you can access the Controller 3000 by providing the correct Login Name and Password. The password protection insures only authorized users access the Controller. We recommend that you change the default username/password. You can restore the factory default password with a hard reset if you forget your password.



Screen 3 Login Screen

Login Enter a valid Login Name here. The default Login is "**root**".

Password Enter the password in this field. The characters keyed-in will be displayed as asterisks (*) to maintain the secrecy of the password. The password entered in this field is specific to the user name entered above. The default password is "**root**".

Get Started After entering the user name and password, click on this button. The user name and password will be validated. If a correct user name and password has been supplied you will gain access to the Controller; otherwise an error message will be displayed.

After successful login, the Controller displays the following screen, which gives the Controller status and allows the user to navigate to different menus of the Controller 3000.

Screen 4 Home Page

Configuration Menus

The Controller 3000 has ten menus. The first eight of the menus deal with configuration of the Controller settings. They are,

1. Express Setup
2. Networks
3. Security
4. Customization

5. Management
6. Advanced
7. System Status
8. System Tools
9. Help
10. Index

These menus allow the user to configure the settings. To access the menu, click on the respective menu button. The ninth menu is Help. It contains Frequently Asked Questions to help the user to understand the system better.

The tenth menu is the index. This menu contains quick links to other menus and sub-menus, to navigate through the interface quickly.

The final option is **Apply Changes/Restart**. Click this from any menu to implement the changes made to the settings. This restarts the controller immediately. You must select **OK** on each page that you wish to configure.

Navigation Menu

The Navigation Menu is available on the top pane of every menu as tabs for accessing different sub-menus of the respective menu. To access the sub-menus, click on the respective sub-menu name.

Status Bar

The Status Bar below the screen will indicate the actions performed.

Cancel and **OK**

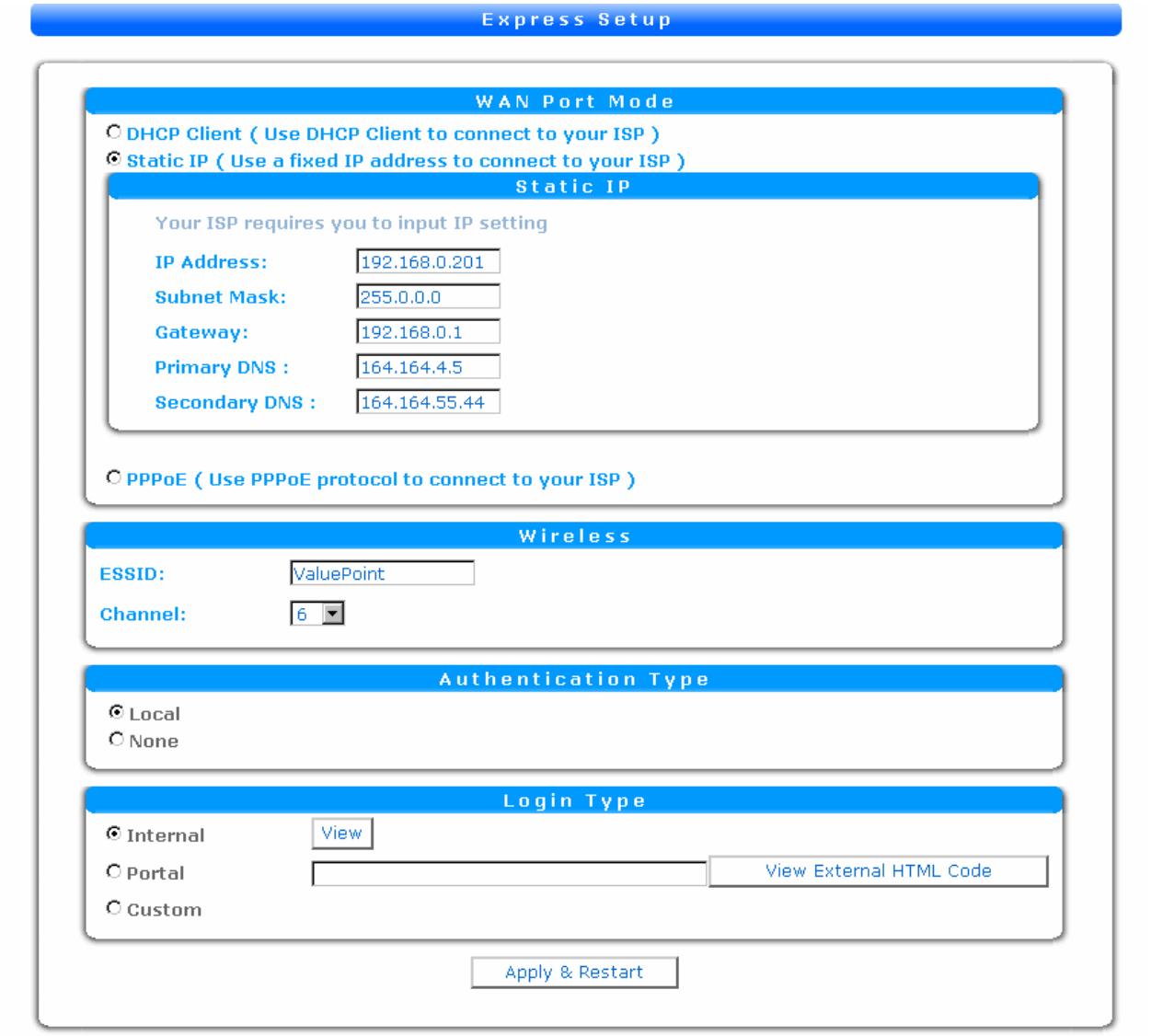
The command buttons **Cancel and OK** can be seen in many menus of the Controller. In all the menus, the functionality of these commands is the same.

Cancel – Click this button to cancel any changes on the current page.

OK – Clicking this button causes the settings configured by the user to be saved. New settings may take effect immediately or on the next reboot.

3.2.2. EXPRESS SETUP

This menu allows the user to configure the basic settings for accessing the Internet.



Screen 5 Express Setup

WAN Port Mode

In this section, select **DHCP Client**, **Static IP** or **PPPoE** setting options.

1. To connect via a Cable Modem or Local LAN select **DHCP Client** setting. This configures the device to obtain the IP address and other TCP/IP settings from your ISP.

2. To use a static IP address assigned by your ISP, or use local LAN settings, select **Static IP** and perform the following steps:
   1. Type the **IP Address** provided by your ISP.
   2. Type the **Subnet Mask Address** provided by your ISP.
   3. Type the **Gateway Address** provided by your ISP.
   4. Type the **Primary and Secondary DNS** server addresses provided by your ISP.

3. To use PPPoE protocol to connect to your ISP, select **PPPoE** and perform the following steps:
   1. Type the **User Name** for PPPoE protocol to connect the ISP.
   2. Type the correct **Password** for the above **User Name**.
   3. Select either **Enable** to activate Auto Connection or **Disable** to deactivate the Auto connection option.
   4. Select the Number of Minutes for **Auto Disconnection** from the drop-down list box.

Wireless

Type the value for **ESSID**. Also, select the **Channel** for the wireless network from the drop down list box here. The values of the drop down are from 1 to 11.

The Express Setup Page has a command button to apply all these settings and restart the Controller. Click **Apply & Restart** to implement the settings.

3.2.3. NETWORKS

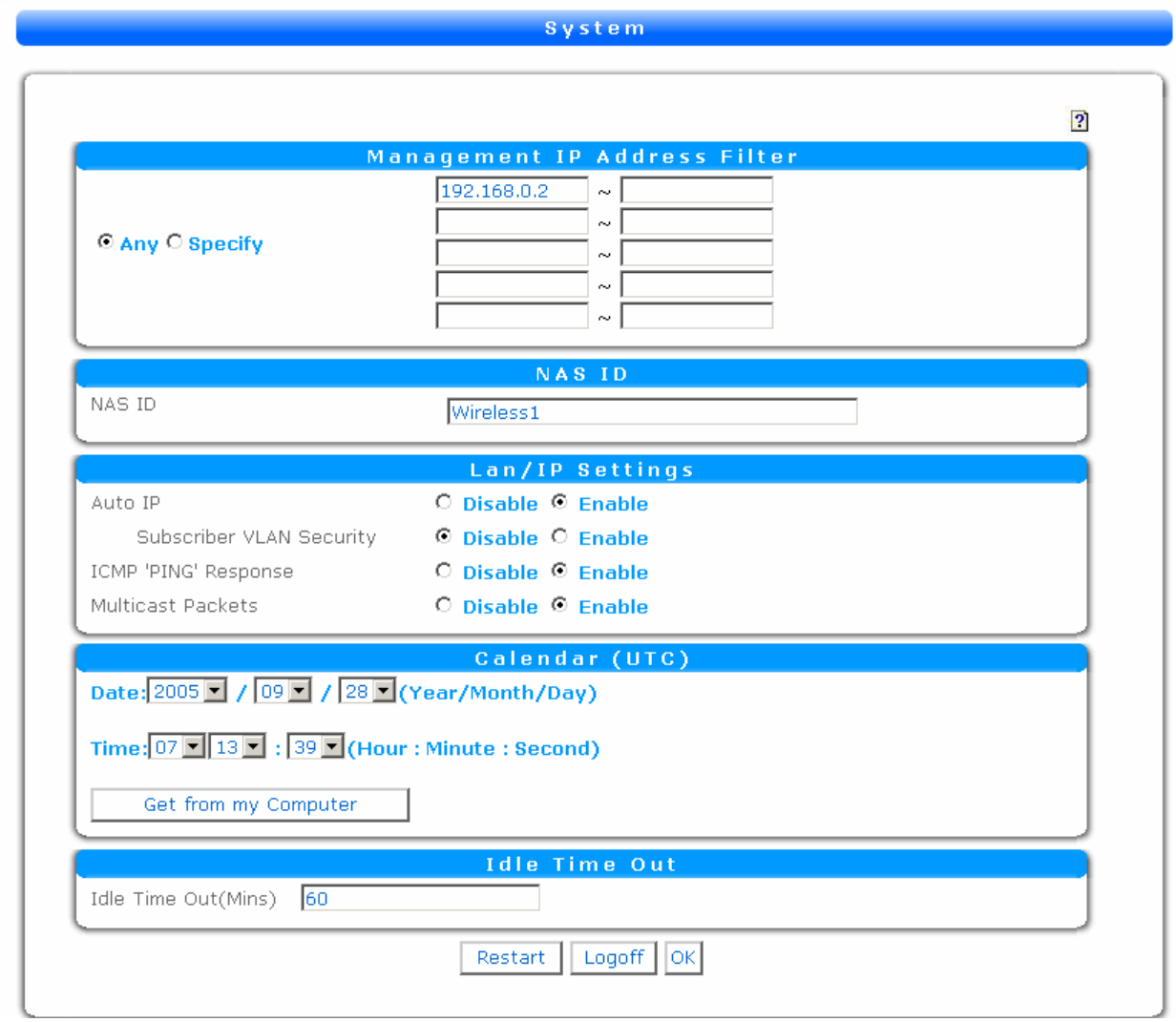
The Networks menu has four sub-menu tabs,

1. System
2. WAN/LAN
3. Server
4. Wireless (WC-3000 Only)

Details of the above menus are as follows,

1. SYSTEM

This section of the Controller allows you to configure the System Settings. The following screen shows the System Settings menu.



Screen 6 System Settings

Management IP address Filter

Select either **Any** or **Specify** radio buttons, to type the access IP address. By default, **Any** IP Address will be selected. The typed IP Addresses should not exceed 15 characters. When **Specify** is selected, only addresses within that range will be able to manage the Controller. Do a hard reset to factory defaults if you forget what addresses are allowed.

NAS ID

The editable text box is the NAS ID of the Controller. This value will be sent in RADIUS Requests from the Controller to the RADIUS Server. If Syslog is enabled, the NAS ID is sent as part of the syslog messages.

LAN IP settings

Auto IP In this section, select either **Enable** or **Disable** radio button to enable or disable the Auto IP subscriber address support. Auto-IP will allow users with Static IP addresses to connect to the internet normally without changing their settings. These subscribers' connections may be slower than DHCP subscribers' due to the translation process to and from their static IP address by the Controller for each packet.

Subscriber VLAN Security (requires Auto-IP enabled) When Subscriber VLAN Security and Auto-IP are enabled the Controller prevents subscribers and other machines on the network from being able to access each other or share resources, using Microsoft Networking for example. You will not be able to access or manage local machines or access points on the LAN with Subscriber VLAN Security enabled. Subscriber VLAN Security is also effective at blocking subscriber-to-subscriber traffic not connected directly to the Controller with some limitations:

1. LAN Broadcast traffic is not blocked, so some subscribers may see other computers listed under "Computers Near Me" in Windows. These subscribers will not be able to share files, ping, or access each other's computers, however.
2. The first "PING" attempt between subscribers may succeed if the Controller has not previously seen traffic from that subscriber. Subsequent PING or other packets will be blocked.

3. Subscriber VLAN Security may not be effective across a switch or router. In this case, direct packets between subscribers cannot be detected by the Controller. If this switch-based configuration cannot be avoided, ValuePoint recommends turning on Subscriber VLAN Security in the Access Points. This feature is available in the SuperAP 500 and 510g products from ValuePoint. Please contact your Access Point vendor with questions about Subscriber VLAN Security in other products.

ICMP Ping Response In this section, select either Enable or Disable radio button to enable or disable the user's access to ping the device. By default, the Controller sets this option to Enable.

Multicast Packets In this section, select either **Enable** or **Disable** radio button to enable or disable the Multicast Packets. By default, the Controller sets the Multicast Pass-through as **Disable**.

Calendar(UTC) This section has drop-down boxes for Date and Time. Select the Date and Time in UTC, from the drop down list boxes as shown in the screen 5. In addition, the user can fetch the system date and time from the computer by clicking on **Get from my Computer**. The selected date and time range should be between ***1/1/2002 to 12/31/2035 and 00:00:00 to 23:59:59*** respectively. Date and Time are stored in the controller as Coordinated Universal Time (UTC/GMT). You must click **OK** on this page to set the internal clock.

Note: Use the 'Get from my Computer' feature the first time you configure the Controller to ensure that the correct local time is set.

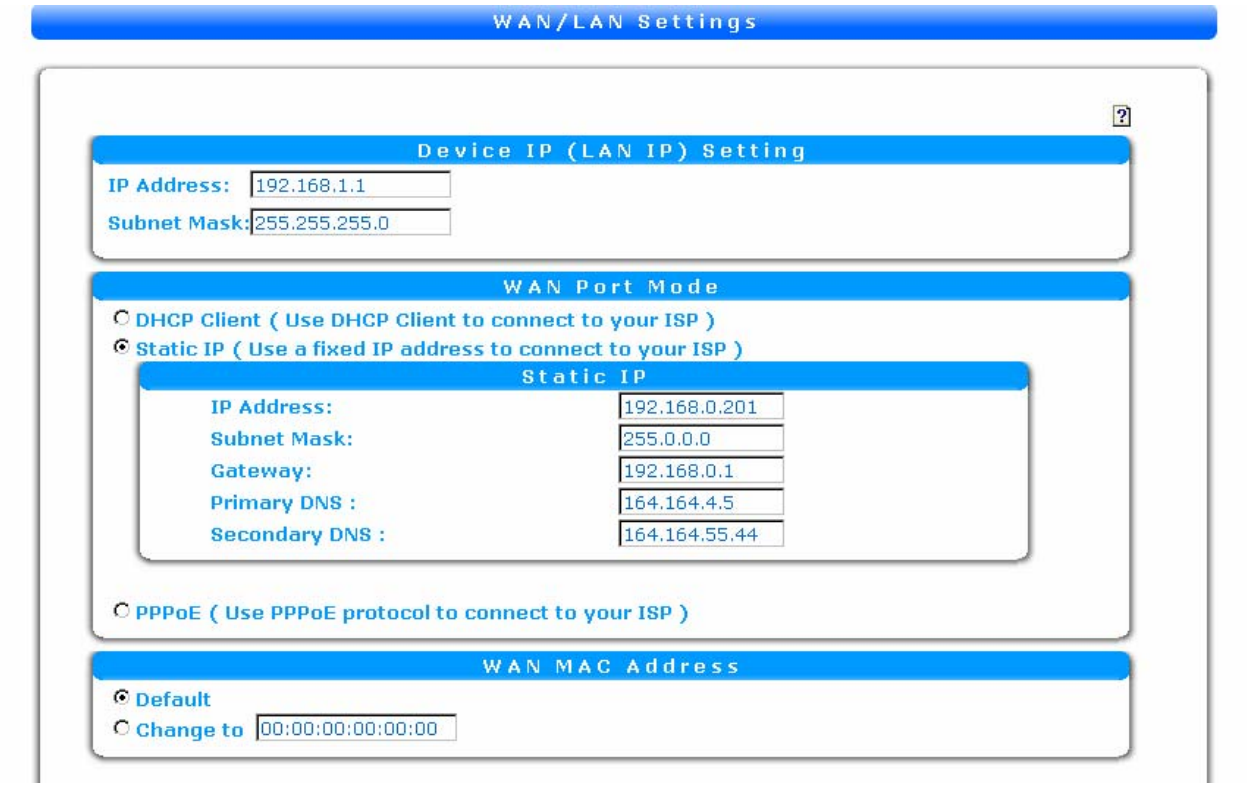
Scheduled Reboot You can configure the Controller to reset automatically every day or **X** days at **XX:XX** time. Keep in mind that the time is UTC/GMT time, so if you want to reboot at 4AM local time make the conversion. This can be useful if you find you have to reset the Controller at a particular site due to unusual subscriber activity.

Idle Time Out(Mins) In this section, select a time out period for inactive subscribers to be disconnected. Enter '0' for no timeout of subscribers. Subscribers who have an active 'logout' pop-up window open will not be timed out.

Note: Setting Idle Timeout to '0' is not recommended for public networks. Unless these subscribers manually log out, their sessions will never be terminated.

3. WAN/LAN

This Menu allows you to configure the WAN/LAN settings of the Controller 3000.



Screen 7 WAN/LAN Setting

Device IP (LAN IP) Setting

Type the IP Address and Subnet Mask of your Controller 3000 here. By default, the Controller sets the value ***192.168.1.1*** as IP Address and ***255.255.255.0*** as Subnet Mask.

WAN Port Mode

Select among **DHCP Client**, **Static IP** or **PPPoE** Port Mode options here to indicate the WAN Port Mode. By default, the Controller selects **DHCP Client** as the port mode.

1. To connect via a Cable Modem and LAN with DHCP select **DHCP Client** Port Mode.

2. To use a static IP address assigned by your ISP or static WAN address select **Static IP** and perform the following steps:

1. Enter the Static IP Address of the Controller.
2. Enter the Subnet Mask for the Controller.
3. Enter the Default Gateway Address.
4. Enter the Primary DNS Number.
5. Optionally, enter the Secondary DNS Number.

3. To use PPPoE protocol to connect to the ISP select **PPPoE** Port Mode and perform the following steps:

1. Enter the User Name for PPPoE protocol provided by the ISP.
2. Enter the correct Password.
3. Select either **Enable** to activate Auto Connection or **Disable** to deactivate the Auto connection option. When Auto Connection is enabled, the Controller will establish a PPPoE session automatically, regardless of subscriber activity. By default, the Controller sets **Enabled** as the value for Auto Connection.
4. Select the Auto Disconnection duration in minutes from the drop down list here. Auto Disconnection will close the PPPoE session if there is no user activity. By default, the Controller selects ***5 Minutes*** as duration.

Subscriber Bandwidth Limit(3500 only)

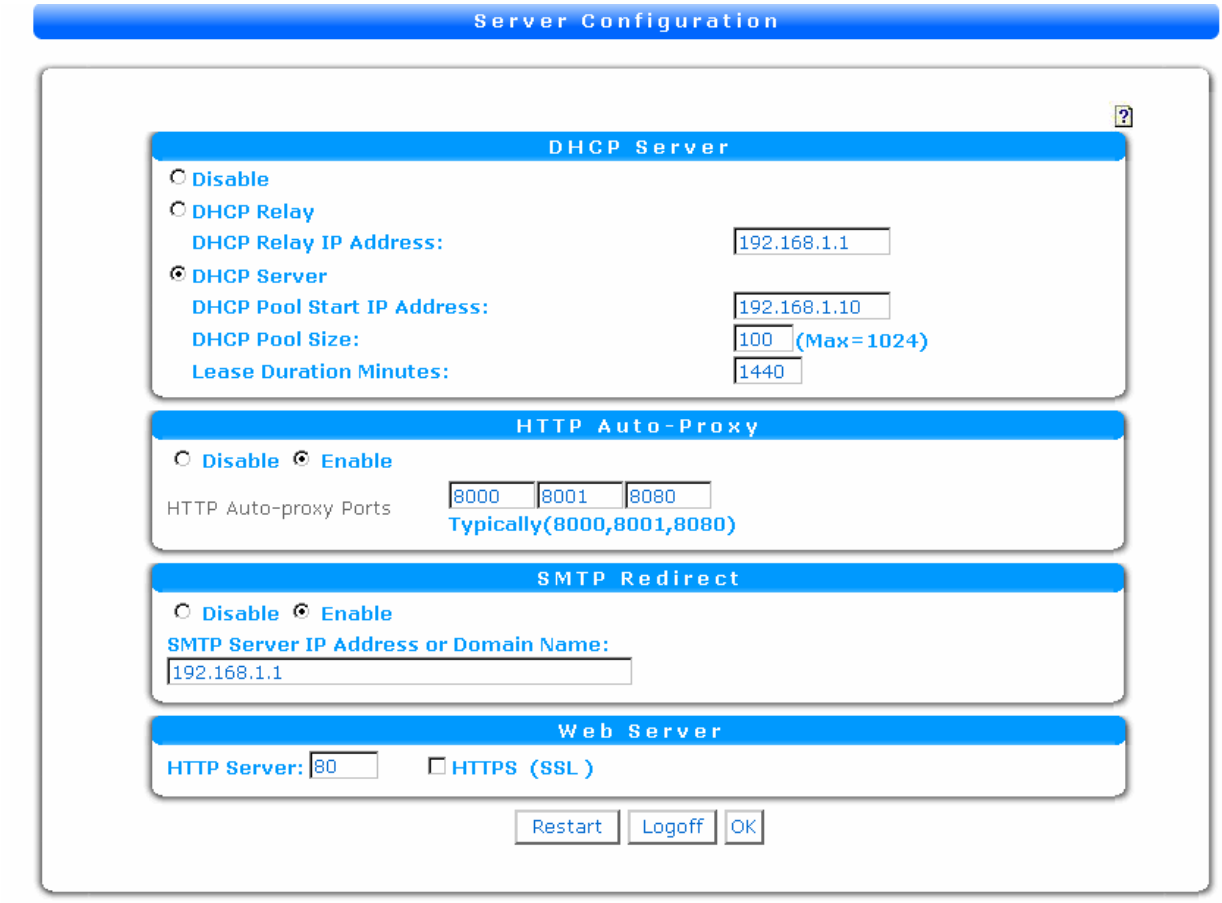
Select **Enable** and **Limit Per Subscriber** to apply a bandwidth limit to each subscribers connection.

WAN MAC Address

Select either **Default** WAN MAC Address or **Change to** option and type the respective WAN MAC Address of the network interface card here. By default, the Controller selects **Default** as the value. This feature can be used if your ISP requires a particular MAC Address to provide service.

4. SERVER

This menu allows you to configure the various Server Settings of the Controller 3000.



Screen 8 Server Configuration

DHCP Server

Select the DHCP Server type you want by selecting the respective radio button here. The available options are **DHCP Disable, DHCP Relay** and **DHCP Server**. The default selection is **DHCP Server**.

1. To disable DHCP server, select **DHCP Disable** option.

2. To enable DHCP Relay, select the **DHCP Relay** option. This will allow the Controller to relay DHCP requests to another DHCP server. The DHCP addresses assigned by that Server will be relayed to subscribers. You will need to configure the following settings:
   A. Type the DHCP Relay IP Address in the text box.
3. To enable the DHCP Server on the Controller, select the **DHCP Server** option. You will need to configure the following settings:
   A. Type the DHCP Pool Start IP Address in the provided text box labeled **DHCP Pool Start IP Address**.
   B. Type the DHCP Pool Size in the text box labeled **DHCP Pool Size**. The size should be between 1 and 253. By default, the DHCP pool is ***100***.
   C. Type the Lease Duration in minutes in the text box labeled as **Lease Duration Minutes**. By default, the lease duration is ***8440***.

Note: You will need to match the IP Pool settings with the Controller LAN settings to insure that DHCP subscribers can connect successfully. You will receive a warning if the settings do not match, but the settings are not changed automatically.

HTTP Auto-Proxy

In this section, you can enable HTTP Auto-Proxy. HTTP Auto-Proxy will detect HTTP Proxy requests from the browser on the LAN and redirect them to a valid Internet connection. Subscribers may find their connection to be slower using Auto-Proxy, so disabling an invalid proxy setting is the best subscriber configuration.

HTTP Auto-Proxy Ports Type the HTTP Proxy Server Ports here. The HTTP Proxy will redirect outgoing connections on these ports. By default, the server ports are ***8000, 8001, and 8080***. These are the typical HTTP Proxy ports used by subscribers.

SMTP Redirect

Enable or **Disable** the SMTP Server redirect. SMTP redirect sends subscriber email to a SMTP server that you designate. This will allow subscribers who are away from their normal

corporate or home network to send mail successfully. The redirect process is transparent, so subscribers do not notice any difference. By default, SMTP redirect is **Disabled**.

SMTP IP Address or Domain Name Provide the SMTP Server address that you wish to direct email traffic to here.

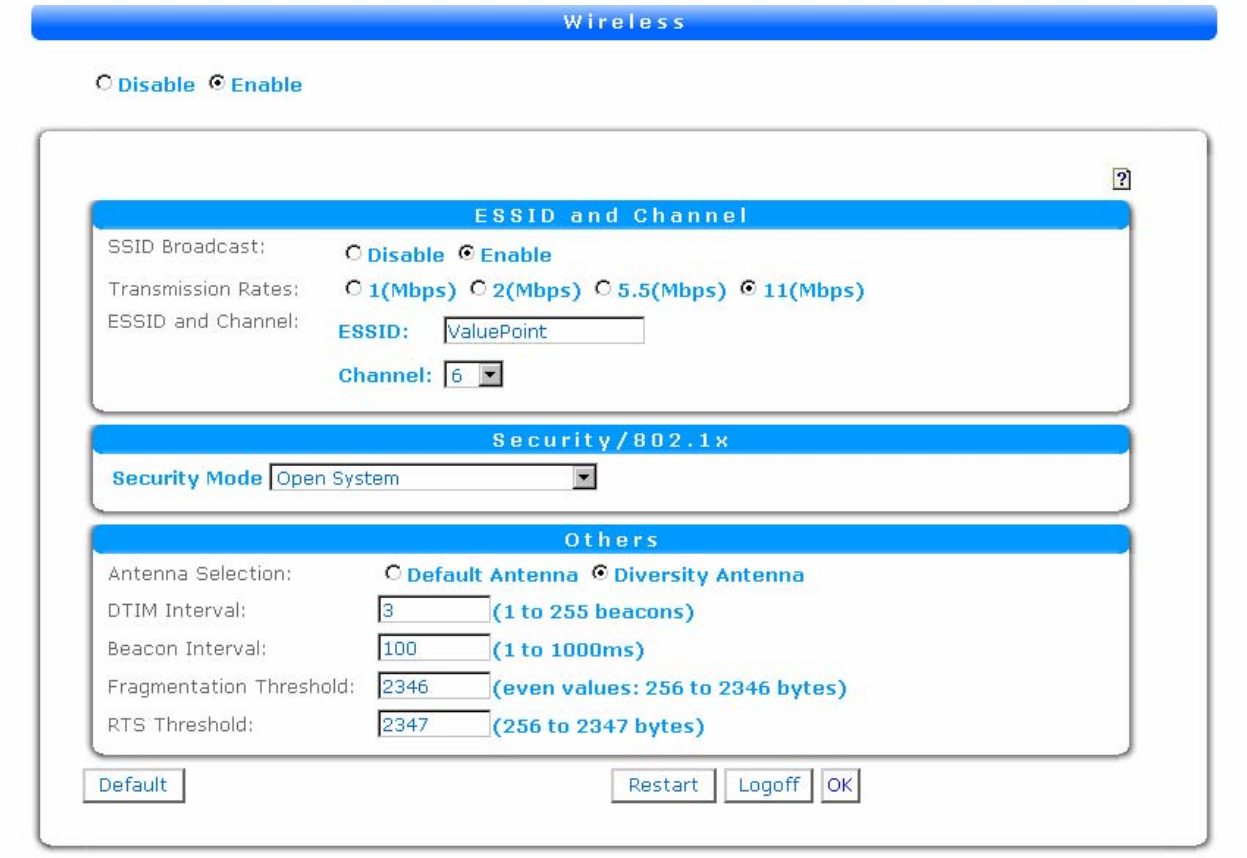
Web Server

HTTP Server Type the Web Server Port here. By default, the port number is ***80***.

SSL Security Check the **SSL Security** check box to enable the SSL Security feature. Enabling SSL will cause WEB GUI and Local Login pages to be encrypted, but may slow down access to those pages. Authenticated users will not see any difference in page load times. By default, SSL Security is not enabled.

5. WIRELESS (WC-3000 ONLY)

This menu allows you to configure wireless settings on the Wireless Controller 3000.



Screen 9 Wireless

Enable / Disable The Wireless Interface of the Wireless Controller 3000 can be enabled or disabled. The Network Controller 3000 will always show disabled. Disabling the wireless LAN will improve the performance of the WC-3000, and it is a good idea to disable the wireless when upgrading the firmware to prevent any unexpected subscriber activity from interfering with the upgrade process.

ESSID and Channel

SSID Broadcast Select Enable and Disable for SSID broadcast. By default, SSID Broadcast is enabled. When SSID is disabled subscribers will not see the network when they scan the area. Subscribers can still enter the network name manually into their WiFi client software.

Transmission Rates Select the maximum Transmission Rate. Setting a lower transmission rates can reduce administrative overhead and prevent users with a stronger signal from monopolizing the network.

ESSID Enter the Service Set Identifier here. By default, the SSID is set to ***ValuePoint***. The SSID is the network name that the subscriber will see when they scan the area for wireless networks. The SSID consists of alphanumeric characters with no spaces. You can create more interesting SSIDs using underscores "_", e.g. "my_network". Spaces in the SSID is not supported.

Channel Select the WiFi radio channel from this select box. You can select a value between ***1 and 11***. In 802.11b channels 1, 6, 11 are the non-overlapping channels. WiFi signals separated by fewer than 4 channels will cause interference and increased 'noise' with each other, lowering connection speed and quality.

Security/802.1x

Security Mode Select the Wireless Security Mode from the drop down list here. Wireless Security protects subscriber data as it is transmitted to and from the Controller WLAN interface.

The wireless security options are

Open System
64-Bit WEP
128-Bit WEP
802 .1x EAP –MD5 No Encryption
802 .1x EAP –MD5 + 64-Bit WEP
802 .1x EAP –MD5 + 128 Bit WEP
802 .1x EAP –TLS No Encryption
802 .1x EAP –TLS + 64-Bit Key
802 .1x EAP –TLS + 128Bit Key

1. To disable Wireless Security select **Open System**. This is the default option.
2. To enable Wired Equivalent Privacy (WEP) select **64-Bit WEP** or **128-bit WEP**. You can provide up to 4 hexadecimal (characters 0-9,A-F) encryption keys. Only one key can be selected at a time. All clients must have the exact same key as the current Controller key (1-4) to connect to the Controller Radio. The default 64/128bit WEP key values are **1111111111** and **11111111111111111111111111**.
3. In order to use 802.1x you need to configure both the individual subscriber's 802.1x client and an 802.1x server. Please see the documentation for your 802.1x client and server for information on establishing an 802.1x session. There are several 802.1x configurations you can use depending on your client and server:
   a. **MD5 / TLS**. MD5 and TLS are two methods of securing the authentication process. You will need to configure this according to your 802.1x server and client settings.
   b. **WEP / Dynamic Keys**. You can use standard WEP to provide wireless security with matching keys on the

subscriber and Controller. Most 802.1x servers can also provide a rotating set of WEP keys, which prevents exploitation of some known WEP weaknesses. If your 802.1x server supports this key rotation, select **Key Rotation** and the **Re-keying Period** in seconds.

Note: 802.1x will not work without extra software configured on each and every subscriber and an 802.1x server in the back office. The Controller just facilitates this connection; it does not provide any 802.1x services by itself.

Others

Antenna Selection This section has two radio buttons: **Default Antenna** and **Diversity Antenna**. By default the Controller is set to **Diversity Antenna**. Diversity antenna may improve detection of weak signals by allowing the Controller to compare the signal from both antennas. If you are going to use a single external antenna, select **Default Antenna** and connect your antenna to the connector labeled 'Tx'.

DTIM Interval Type the DTIM Interval here. The Interval should be between ***1 and 255***. By default, the value is ***3***.
This setting, a multiple of the beacon period, determines how often the beacon contains a Delivery Traffic Indication Message (DTIM). The DTIM tells power-saving client devices that a packet is waiting for them.

Beacon Interval The Beacon Interval should be between ***1 and 1000***. Beacon Interval is the frequency of the WiFi Beacon broadcast that informs wireless subscribers of the SSID and other administrative information.

Fragmentation Threshold Type the Fragmentation Threshold here. The Threshold should be between ***256 and 2346*** and only even numbers can be entered here. By default, the fragmentation threshold is ***2346***.

This setting determines the size at which the packets are fragmented. You can use a lower setting in areas where communication is poor or where there is a great deal of radio interference.

RTS Threshold Type the RTS Threshold here. The Threshold should be between ***256 and 2437***. By default, the RTS threshold is ***2432***.

This setting determines the packet size at which the Controller 3000 issues a request to send (RTS) before sending the packet. A low RTS Threshold setting can be useful in areas where many client devices are associating with the Controller 3000, or in areas where the clients are far apart and can detect only the Controller 3000 and not other wireless subscribers.

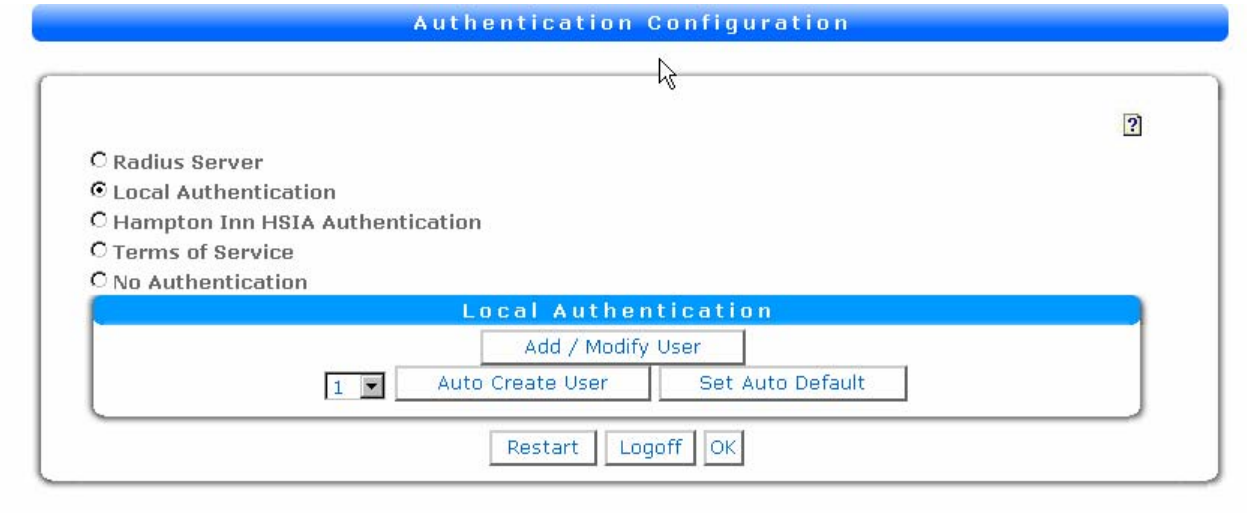
Default

Default Values for wireless settings are restored**.**

3.2.4. SECURITY

1. AUTHENTICATION

This menu allows you to configure the Authentication Settings of the Controller 3000.



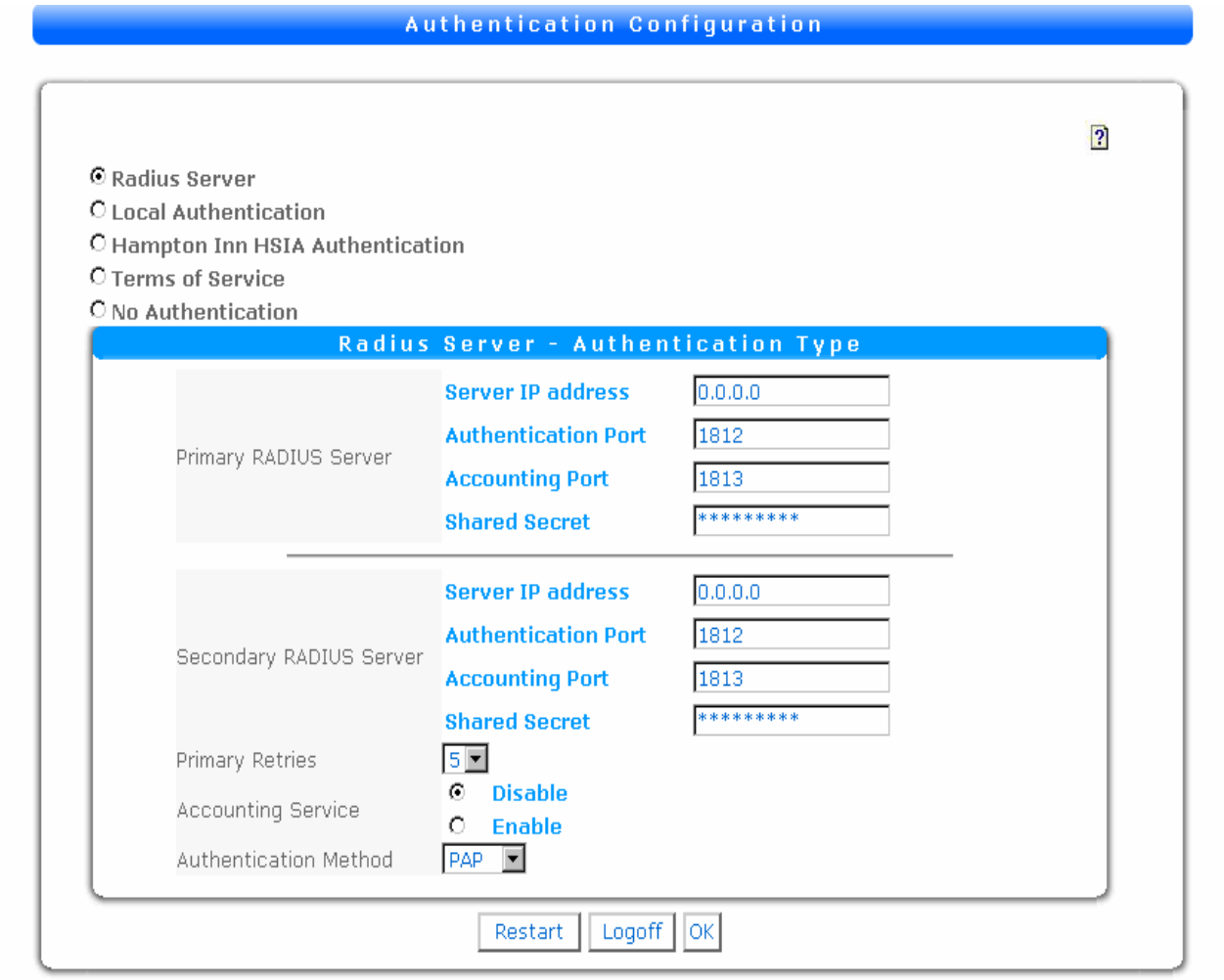
Screen 10 Authentication Configuration

The Authentication Configuration has five radio button options: **RADIUS Server**, **Local Authentication**, **Hampton Inn HSIA Authentication, Terms of Service** and **No Authentication**. By default, **Local Authentication** is enabled.

RADIUS Server

Remote Authentication Dial-In User Service (RADIUS) is an authentication and accounting service used by many service providers to track and control subscriber access. The Controller includes a RADIUS Client that can be configured to make RADIUS requests when subscribers authenticate. RADIUS Authentication requires a RADIUS Server in the back office in addition to the RADIUS Client.

If the **RADIUS Server** option is selected the RADIUS specific settings are displayed:



Selecting RADIUS Server option Window

The configurable options on this menu are:

Authentication Type

Primary RADIUS Server The Primary RADIUS Server provides the authentication and accounting for subscribers. When the subscriber enters their username and password, these parameters and other are sent to the RADIUS Server. The RADIUS server then responds back to the Controller with an 'accept' or 'reject' message. The Controller enforces the authentication decision made by RADIUS. To configure the Primary RADIUS Server configure these values:

1. Primary RADIUS Server IP Address.
2. Primary RADIUS Server Authentication Port Number. By default, the value is ***1812.*** This is the typical Authentication port, but your server may be different.
3. Primary RADIUS Server Accounting Port Number. By default, the value is ***1813***. This is the typical Accounting port, but your server may be different.
4. Primary RADIUS Server Shared Secret Key. The Shared Secret Key should not exceed 15 characters. The same key must be entered into your RADIUS server.

Note: Your RADIUS Server may require additional information beyond the Shared Secret to accept RADIUS requests from the Controller. Common requirements are the NAS ID and IP Address of the RADIUS Client. Please consult your RADIUS Server documentation for more information on connecting RADIUS Clients.

Secondary RADIUS Server The secondary RADIUS Server has the same configuration options. This RADIUS Server will be contacted if the Primary fails to respond.

1. Secondary RADIUS Server IP Address.
2. Secondary RADIUS Server Authentication Port Number.
3. Secondary RADIUS Server Accounting Port Number.
4. Secondary RADIUS Server Shared Secret Key.

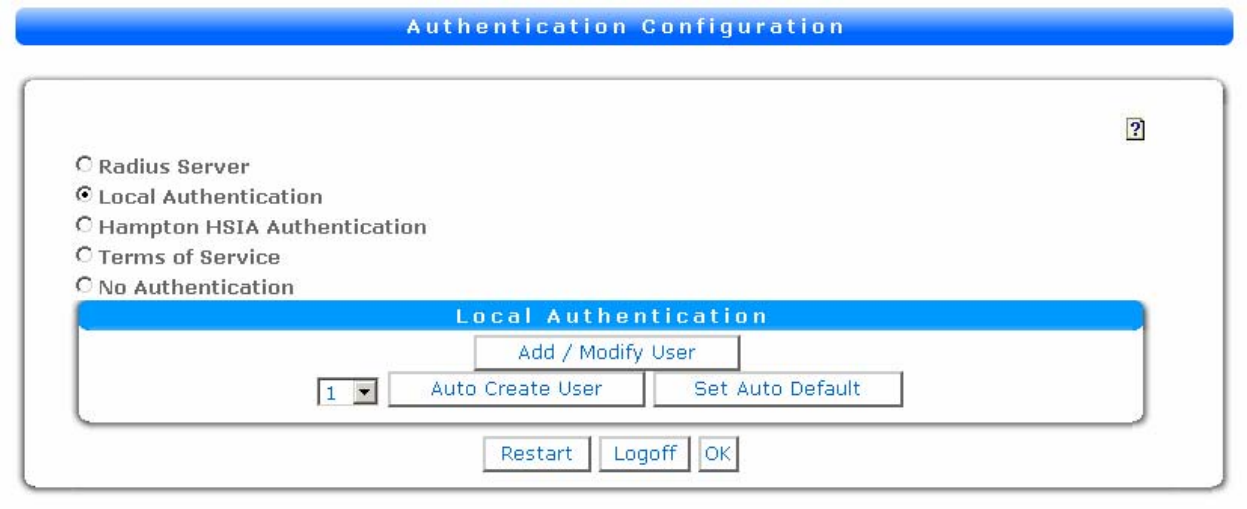
Retry Times when Primary Fails Select the Number of Retries the Controller should make when the RADIUS Server fails from the drop down list box. After the selected retries on the Primary Server the Controller fails over to the Secondary Server. The Controller aborts the authentication request and returns an error after all retries fail against the secondary RADIUS server.

Accounting Service You can **Enable** or **Disable** Accounting Service here. Turning on accounting causes the Controller to send a summary of subscriber activity to the RADIUS server.

Authentication Method Select the Authentication Method for RADIUS from the drop down list box here. The values of the drop down are **PAP** or **CHAP**. PAP and CHAP are two security methods used by RADIUS. Please consult your RADIUS Server documentation for details on which method your Server requires.

Local Authentication

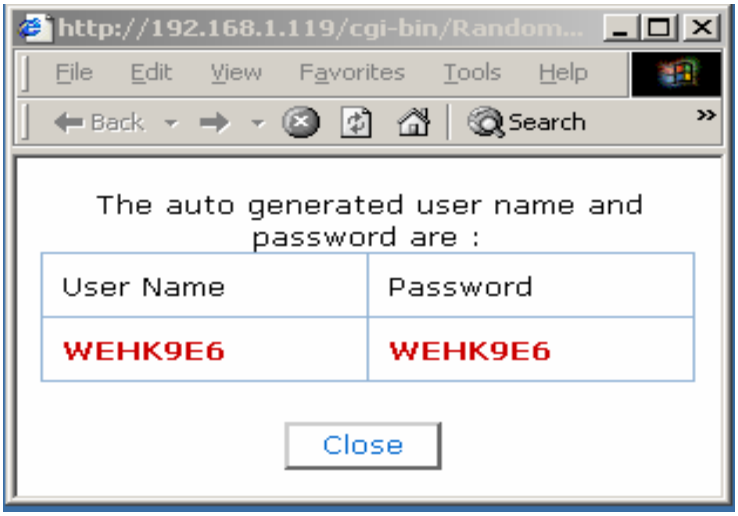
If **Local Authentication** is selected, the menu displays three command buttons. They are, **Auto Create User, Set Auto Default,** and **Add / Modify User**.



Selecting Local Authentication option Window

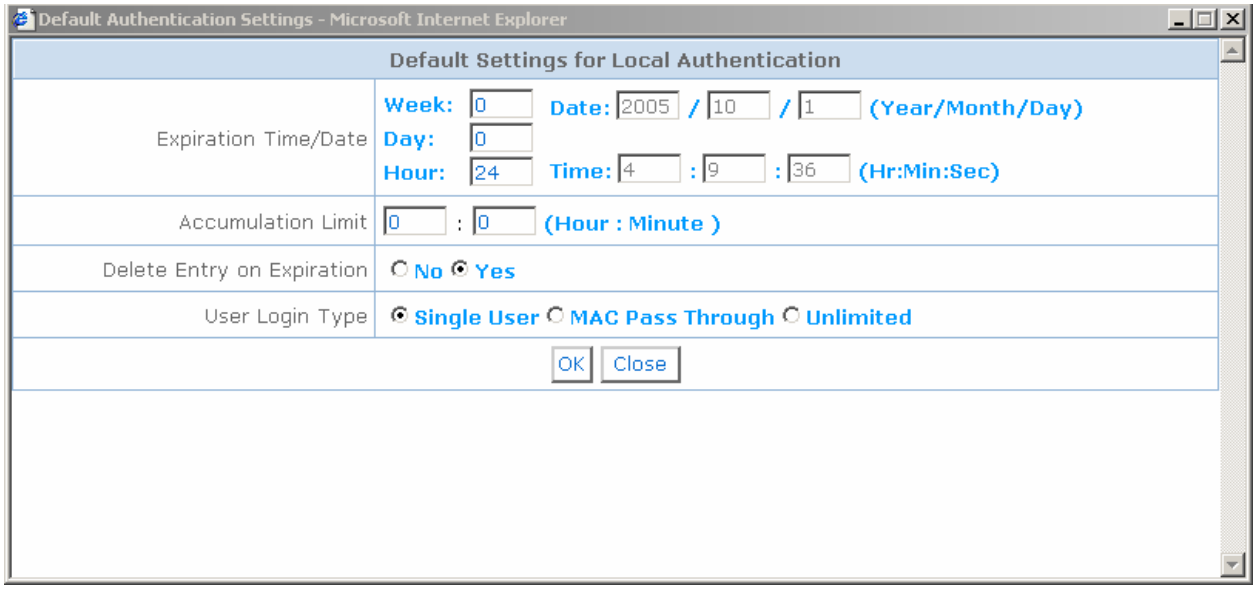
Auto Create User

Click **Auto Create User** to create usernames and passwords automatically. These accounts will have the properties selected under Set Auto Defaults. Indicate the number users to be created by selecting a value from the drop-down list box that is found near to this command button. By default the selected value is ***1***. When the user clicks **Auto Create User** a pop-up window shows the automatically generated usernames and passwords. You can print using the regular browser printing options from this page.



Popup window of Auto Create User command

Set Auto Default Click **Set Auto Default** to set default values to this section. Clicking this command will display a pop-up window with various authentication settings. Use these settings to define the kind of users and time limits to be automatically created. Click **Apply** to implement these settings. It may take a little while to generate a large number of accounts.



Popup window of Set Auto Default User command

Expiration Date/Time Set the amount of time the account should remain valid. **Week**, **Day**, and **Hour** set the duration of the account from today, shown under **Date** / **Time.**

Accumulation Limit Usage limit in minutes of the account. Set to zero for unlimited.

Delete Entry on Expiration This Account will be deleted on the Expiration Date/Time

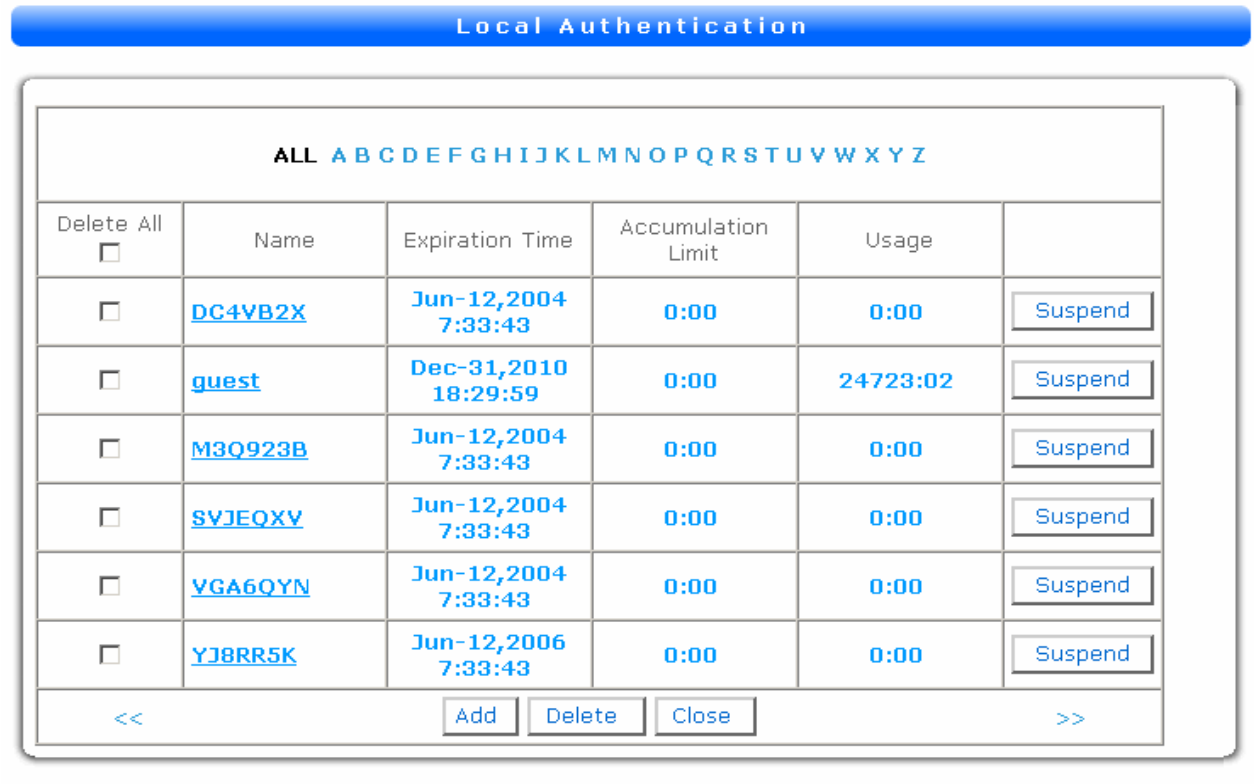
User Login Type Select the User Login Type here. There are three account types. **Single PC – Login** allows only a single computer to access the account by the user logging in each time they connect. Once used the account is locked to that PC based on the MAC address of the network hardware. **Single PC – Mac Address Passthrough** allows a computer to access the

account, but only the first connection requires a login. Future connections are logged in automatically. **Unlimited PCs – Login** allows multiple subscribers to use a single account simultaneously, but they must provide the username/password each time they connect.

Note: A laptop typically has two different MAC addresses for the Ethernet port and the Wifi card. A single PC account will only allow one of these to be used. For example, if a hotel has Ethernet in the rooms and WiFi in the lobby, whichever is used first will lock the Single PC account to that MAC address only.

Add/Modify User

Click **Add/Modify User** to add, delete and modify a user for local authentication. A pop-up window displays the names of all the authenticated persons. The window allows you to add, delete, suspend/resume, or modify the local users. Suspended users will not be able to log in until their account is resumed.



Popup window of Add/Modify User command

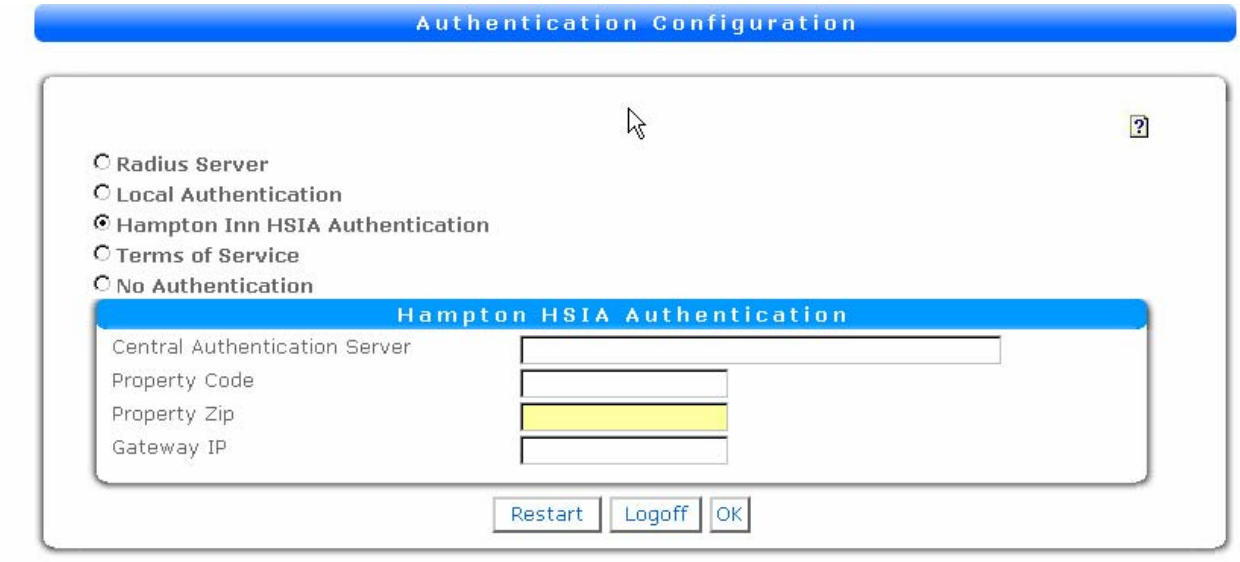
Add Opens a dialogue to add a new user account. See the settings for Set Auto Default User above for setting details.

Delete Remove the checked users.

Edit(click username) Clicking on a username opens an edit window. The options are the same as for adding users.

Hampton Inn HSIA Authentication

To use the Hampton Inn HSIA Central Authentication Server (CAS), select Hampton Inn HSIA Authentication. This will open a dropdown with Hampton specific configurations. The default values are for testing only, please contact Hampton Inn for valid configuration settings for the hotel property you are installing.



Selecting Hampton Inn HSIA Authentication option Window

Central Authentication Server Enter the correct Central Authentication Server (CAS) URL for the Hampton portal page. You will need to provide the correct CAS for subscriber authentication. You must get the Hampton CAS information from Hampton Inn Corporate Office or the Hampton Inn site owner.

Property Code Enter the Property Code provided by Hampton Inn for the property you are installing.

Property Zip Enter the Property Zip Code.

Gateway IP In most cases this field is blank. Normally the Public IP of the Controller will be provided to the CAS automatically. If the Controller is behind a NAT firewall, you can use this field to override this and provide the IP Address of the Firewall here. Configure the NAT Firewall on your router to forward port 1111 to the Controller to enable Hampton Inn HSIA Authentication through NAT.

Terms of Service

To use the **Terms of Service** authentication, select this option. Subscribers will not be able to access the WAN until they click on the "I Accept" button on the terms of service page. You will need to upload an HTML that contains the text of your terms of service and the post-authentication redirect. You can upload this file under **System Tools – Maintenance – Terms of Service**. You can also download the current terms of service file to use as a template.

Configuring the Terms_of_Service.htm file

You can customize the HTML file however you like. Only the POST code must not be changed except the redirecturl field. The default page uses some Javascript to process the POST. If you are replacing or removing this code you must test your pages to make sure your HTML or Javascript is making the POST correctly.

<input type="hidden" name="redirecturl" value=""> The string between the **value=""** field determines the web URL, if any, that the subscriber is redirected to after agreeing to the terms of service. If this field is blank the subscriber will be redirected as configured under **Customization – Login – Default Post-Authentication Default**. For example, if you use **value="**http://www.valuepointnet.com/**",** subscribers will be redirected to ValuePoint after they accept the terms of service.

Note: The Terms of Service text is a legal agreement that is specific to your service. For this reason, ValuePoint Networks cannot provide a standard or boilerplate Terms of Service.

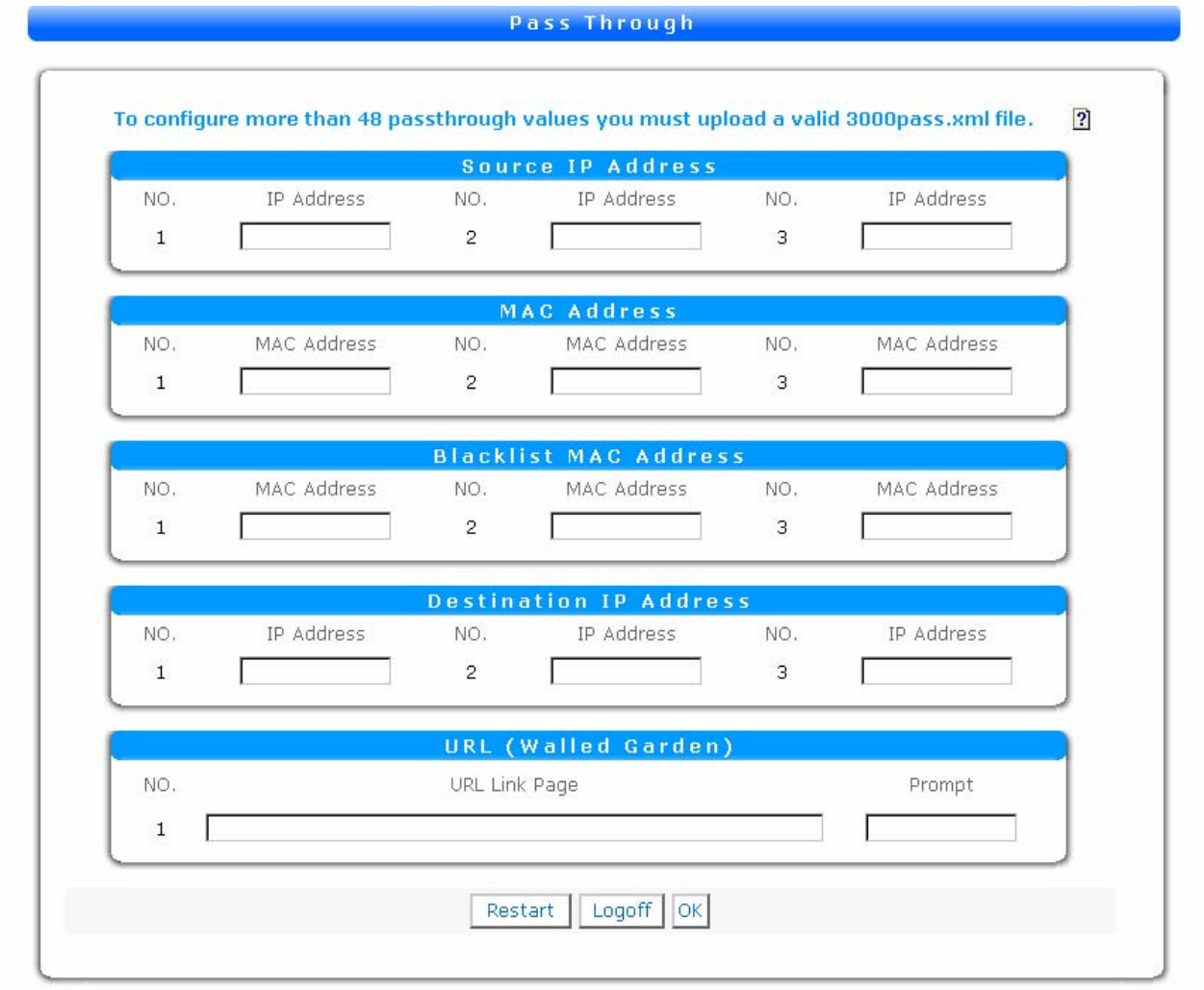
No Authentication

If you do not wish to control subscriber access to Internet, select **No Authentication**. In this configuration, subscribers will still need to initiate a HTTP request by opening their web browser in order to be passed through the firewall. This process is transparent to the subscriber. If subscribers ping or send email before requesting a web page these requests will not go through. In effect, these subscribers are still authenticated for the purposes of logging and tracking usage, blocking banned users, and so forth.

Note: If you need some users to be connected without opening a web browser, or have equipment like security cameras which must remain connected, use the IP Address Passthrough table. These IP Addresses are always connected and not affected by any security setting.

2. PASS-THROUGH

These settings allow you to define the pass-through subscribers and destinations when using Authentication.



Screen 11 Pass-through Menu

There are two options for configuring Pass-through settings in the Controller. If you only need a limited number of entries, up to 48 per option, you can configure these from the GUI directly. If you need to configure more you must use the pass-through XML file **3000pass.xml**. The XML file is uploaded through **System Tools - Maintenance – Pass-through**. It is only necessary to add subscribers to one pass-through table, depending on what kind of connection they require.

Pass-through Source IP Type the Subscriber's pass-through IP Address here. Subscribers or devices with these addresses will be permanently connected. These IP Addresses are not affected by the black list, redirection, or any other connection limitation. You can use this table for equipment like security cameras which must be permanently connected to the internet.

Pass-through MAC Address Type the Subscriber's pass-through MAC Addresses here. Subscribers with these addresses will not be required to authenticate, but must open a web browser to be connected to the internet and are otherwise subject to security settings, advertisements, etc.

Note: As with the No Authentication configuration, MAC Address Pass-through users will need to initiate a HTTP Web Browser connection to be added to the firewall so they can send email, ping, or make other connections through the Controller.

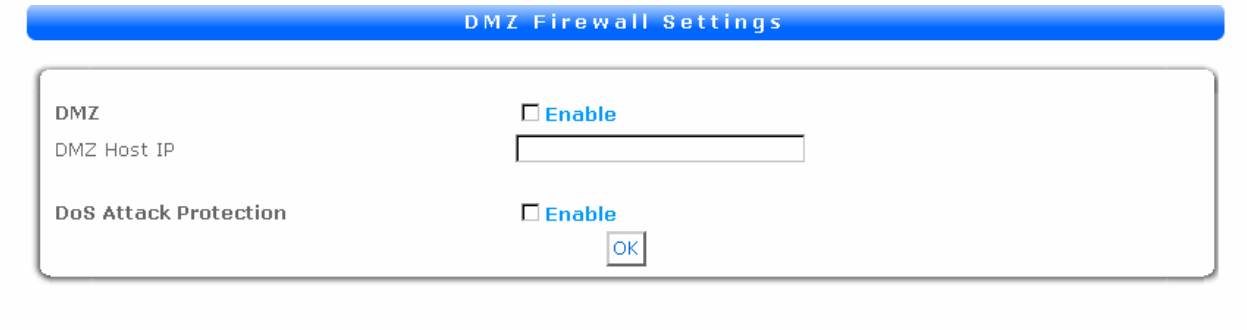
Blacklist MAC Address Type the MAC address of blocked Subscribers here. Subscribers with these MAC addresses will not be able to authenticate.

Pass-through Destination IP Address Type the pass-through Destination IP Addresses here. All subscribers will be able to access these IP addresses without having to authenticate.

Pass-through URL (walled Garden) Type the pass-through Destination URL here. Subscribers will be able to access these web pages without having to authenticate.

Note: Use the pass-through tables to allow access to web resources before the subscriber is logged in. This includes redirect login pages and any images/advertisements on those pages. If you want to redirect on logout add those pages here as well.

3. DMZ FIREWALL



Screen 12 DMZ Firewall

DMZ

DMZ stands for Demilitarized Zone. This section allows the user to specify the IP Addresses for a DMZ server that can be freely accessed through the firewall. All Controller ports are forwarded to this internal address.

Enable Check this to enable the DMZ property.

DMZ Host IP Type the IP Address for which access can be provided.

DoS Attack Protection

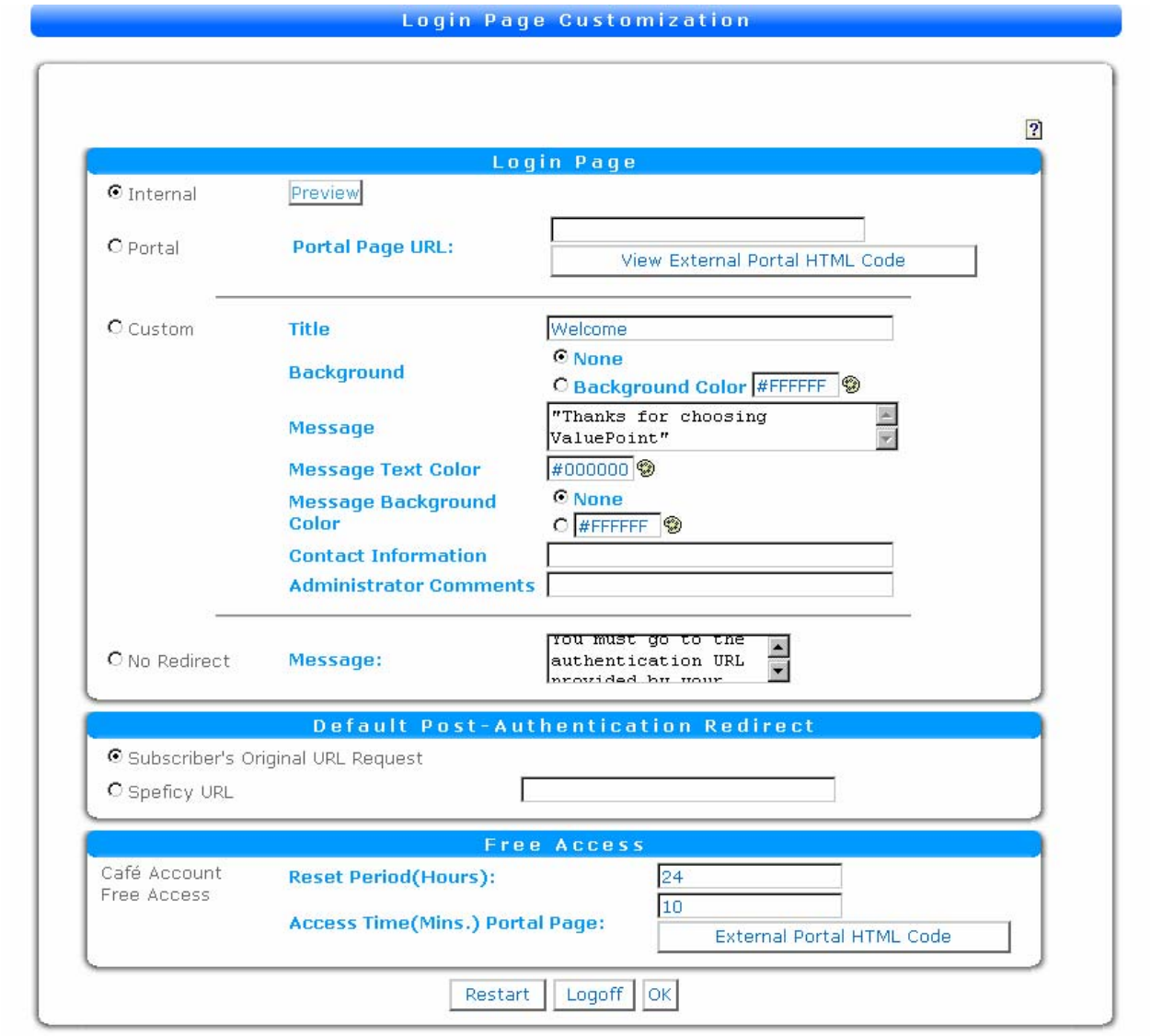
This section allows the user to enable a service that protects the Controller from common remote Denial of Service attacks on the WAN port.

Enable Check this to enable the DoS Attack Protection.

3.2.5. CUSTOMIZATION

1. LOGIN PAGE

This menu allows you to customize the Login Page settings of the Controller 3000.



Screen 13 Login Page

Internal

Select this option to keep the standard default login page. To view the standard Login Page that subscribers will see, click on the **Preview** button. Selecting this option will pop-up a dialog box prompting the user to enter the user id and password to be authenticated.

Portal

Select this option to redirect the Login Page URL to a Web Page hosted outside the controller. In order to subscribers to login successfully, you will need to put the correct HTML POST FORM on your Web Page. To see and cut/paste the required code, click on the **View External Portal HTML Code** button. When you put the HTML code on your portal page do not change the contents of the **<form>** and **<input>** tags. Beyond these tags you can customize the look and feel, and even automate functionality as much as you want. This makes the Portal login page the most popular and common configuration for login pages.

Include Subscriber Information In order to make portal pages more powerful, subscriber and Controller attributes can be inserted automatically into the redirect URL to your portal page. You can use this to identify subscribers and locations on your portal page for special handling. Select **Customization - Login Page - Include Subscriber Information** to enable this feature.

Without Subscriber Attributes selected, your redirect URL produces this in the browser:
http://www.gateway.com/3000/login.html

Selecting Subscriber Attributes produces this in the browser:
http://www.gateway.com/3000/login.html?NASID=NotellMotel&MAC=000BDBDF1DFB&URL=www.google.com

Your portal page can parse these values from the URL:

NASID=[NASID configured under **Networks - System**]
MAC=[Subscriber MAC Address]
URL=[Subscriber's original request URL]

You can use these values in your CGI to provide special handling for subscribers or locations on your portal page. The most common uses are branding each page according to the source venue and redirecting subscribers back to their original request after authentication. Please consult your Web Designer on the use of CGI variables in web server design.

Note: This CGI is appended to the URL request as entered under Portal Page URL. If you have already specified a CGI string using ?, you will end up with two ? characters in the URL. Ensure that your CGI will handle this situation correctly.

Custom

Select this option to customize the text of the Internal Login Page in the Controller 3000.

Title Type the desired Welcome Slogan here.

Background Select the desired Page Background by selecting either **None** or **Background Color** option.

1. If **None** is selected, then the Page Background will be white.
2. If **Background Color** option is selected then the user can further select the desired background color by clicking on the icon given right after the Background Color text box.

Message Type the desired Message, which will appear on the Login Page.

Message Background Color

Select the desired Message Background by selecting either **None** or **Background Color** option.

1. If **None** is selected, then the Message Background will be displayed as white.
2. If **Background Color** option is selected then the user can further select the desired Background Color by clicking on the icon given right after the Background Color field.

Contact Information Type Contact Information for the ISP or Support, if any, here.

Administrator Comments Type the Administrator Comments here, if any.

No Redirect

Select this option to get authenticated using a URL link provided by the service provider. Subscribers must enter this address manually, and it must be included in the **Walled Garden**. When they try to access another web site without authenticating they will receive and error.

Default Post-Authentication Redirect

Subscriber's original URL request Select this option to redirect the subscriber to the original subscriber entered URL after authentication. For example, if the subscriber's home page is www.valuepointnet.com, they will be redirected to the login page, and then redirected again back to their original request after successfully logging in.

Specify URL Select this option to redirect the subscriber to specified URL after authentication. This setting will override any URLs specified in the 3000terms.xml file or Portal Page authentication code. This feature can be used to redirect all authenticated customers to a hotel website, for example.

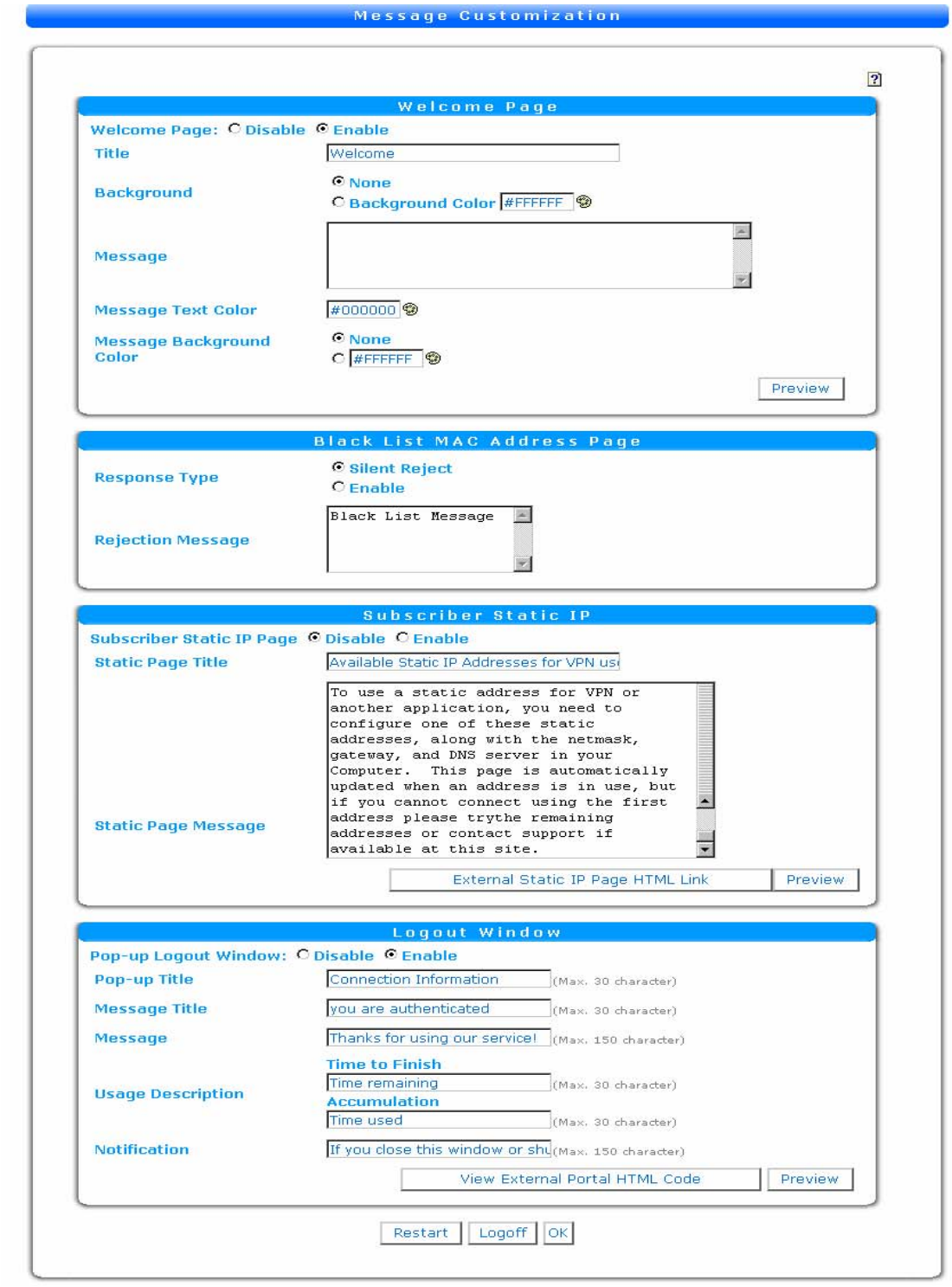
Free Access

You can configure the Café Account™ settings in these fields. This feature allows any subscriber not on the Black List to get limited authentication time. Once their limited time has expired they must wait for the next free access period or log in with a valid username/password. The free access is controlled by MAC address, so a subscriber will not be able to connect again with the same PC until the next period. The values in the first box indicate how often free access is available in hours. The second box indicates the duration allocated for free access in minutes. To allow free access from a redirected or external web page, click on the **External Portal HTML Code** button and cut/paste the HTML code. For example, if you set free access to 30 minutes every 24 hours, this would allow any user to access the internet for 30 minutes once per day. This might be appropriate for a fast food restaurant.

Note: You can disable Free Access, and prevent the prompt from appearing on the Internal Login, page by setting the time to '0' minutes.

2. MESSAGE CUSTOMIZATION

This menu allows the user to customize the message text of the Controller 3000. The message customization screen appears as shown below,



Screen 14 Message Customization

Welcome Page

Subscribers who are configured with pass-through access will not be redirected to a login page. An option welcome page for these subscribers can be configured for these users.

Title The title of the welcome page, which is displayed at the top of the welcome page.

Background Select the desired Page Background Color by selecting either **None** or **Background Color** option.

1. If **None** is selected, then the Message Background will be displayed as white.
2. If **Background Color** option is selected then the user can further select the desired Background Color by clicking on the icon given right after the Background Color text box.

Message Type the Welcome Message, which is to be displayed in the in the welcome page here.

Message Text Color Select the desired Text Color of the message by clicking on the icon given right after the Message Text Color text box.

Message background Color Select the desired background Color for the message by clicking on the icon given right after the Message background Color text box. If no color is needed indicate it by selecting **None.**

Preview When clicked a pop-up window shows a preview screen with the current settings.

Black List MAC Address Page

Response Type Select **Enable** to enable the message to be displayed when a black listed subscriber attempts to connect to the Controller. Select **Silent Reject** to reject connections with no response.

Rejection Message If the response type is **enabled** then type the rejection message here. When a blacklisted MAC address attempts to connect, they will receive this message.

Logout Window

Pop-up Logout Window Select either **Enable** to enable the Pop-up Logout Window or **Disable** to disable the same.

Window Name Type the Logout Window Name here. It accepts up to 30 characters.

Main Message Type the Main Message or Title in this text box. This accepts up to 30 characters.

Message Description Type additional comments or continue Main Message here. This accepts up to 150 characters.

Time Count Label This has two text boxes namely **With Session Timeout** and **Without Session Timeout.** Type the Time Count Label for **With Session Timeout** and **Without Session Timeout** here. They accept up to 30 characters each.

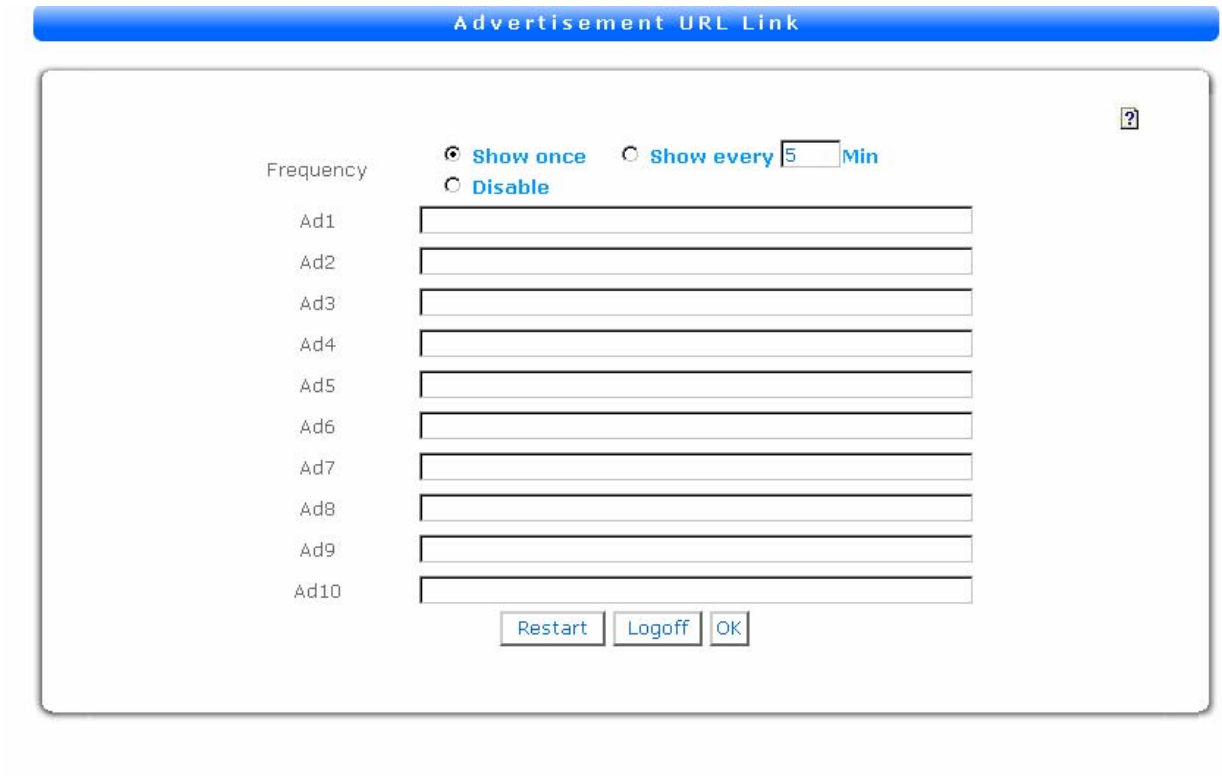
Warning/Alarm Message Type the Warning or Alarm Message here.

Preview When clicked a pop-up window shows a preview screen with the current settings.

Note: The Logout pop-up window generates the automatic advertisements. If you disable the pop-up, you will disable advertisements.

3. ADVERTISEMENT

This menu allows the user to link the Advertisement URL's to the Controller 3000. These will be displayed to the subscriber when they connect and every few minutes as configured.



Screen 15 Advertisement URL Link

Frequency

Select the Frequency at which the Advertisement is to be displayed by selecting either of **Show Once** or **Show Every** or **Disable** option here. The frequency is set in minutes.

If the user has selected **Show Once** option then only the first Advertisement will be displayed once to the subscriber.

If the user has selected **Show Every 'X' min** option then the Advertisements will be displayed at intervals defined by the number of 'X' minutes entered in the adjacent text box. Each advertisement will load in turn.

If the use has selected **Disable** option, Pop-up advertisements are disabled

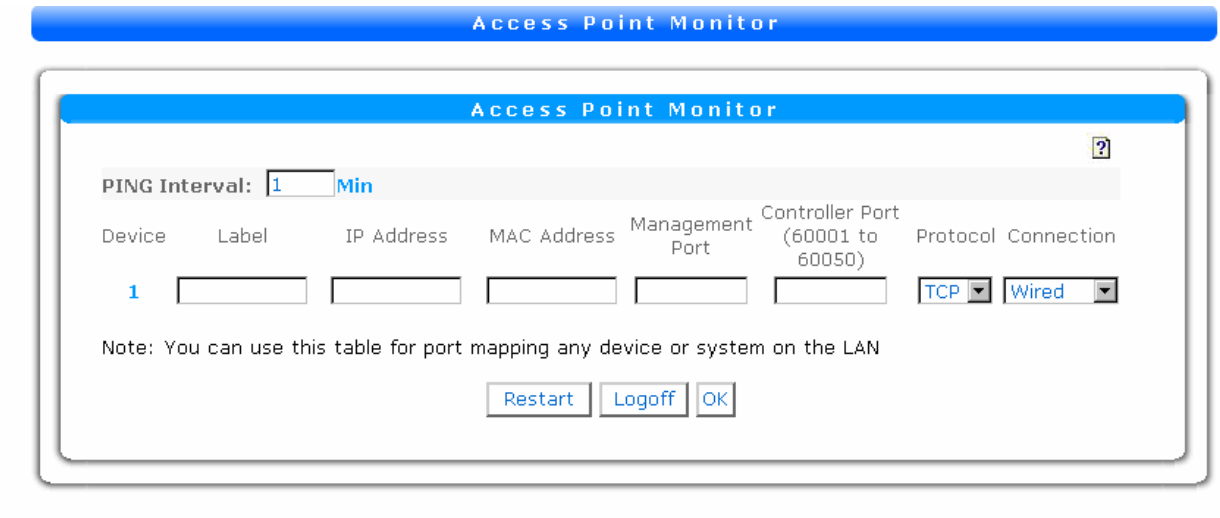
Ad[X] Type the URL Links to the advertisements which are to be displayed.

Note: The Logout pop-up window generates the automatic advertisements. You must enable the logout pop-up if you want to generate advertisement windows.

3.2.6. MANAGEMENT

1. ACCESS POINT MONITOR

This menu allows the user to configure the Access Point Monitor, which will facilitate management of your public access network. The Controller will track the status, online or offline, of these devices, and allow access to their management interfaces through NAT for remote access. You can also use this table to establish port mapping to any LAN address.



Screen 16 Access Point Monitor

PING Interval Type the Detecting Time of the LAN Device here.

Label Type the Device Name here.

IP Address Type the Device LAN IP Address here.

MAC Address Type the Device MAC Address here.

Management Port Type the Virtual Port Number of the Device here. To access the device remotely you connect to the Controller WAN address plus the device Management port. For example, if the Controller is at http://1.2.3.4 and the virtual port is 60001, you could access the Access Point at http://1.2.3.4:60001.

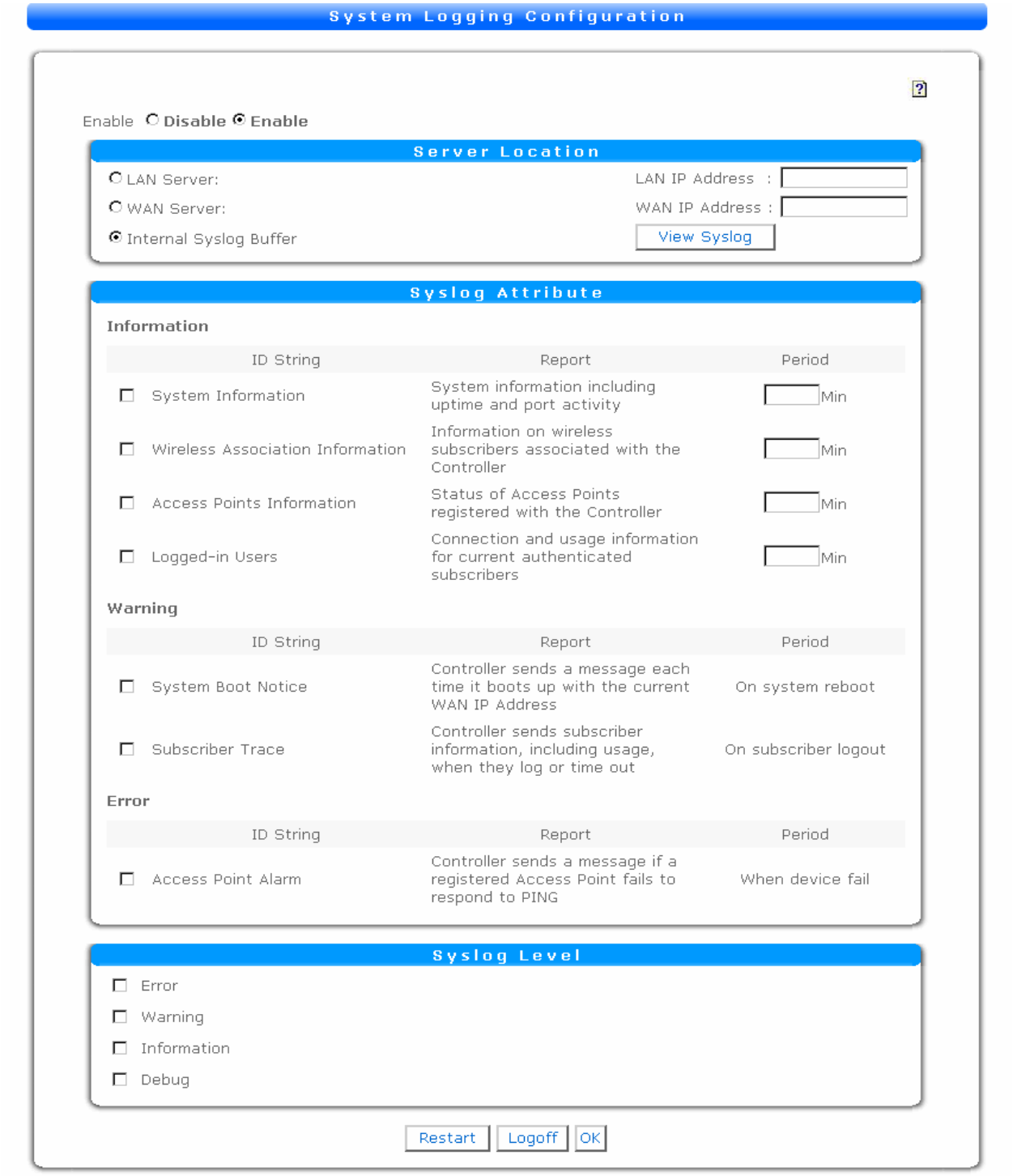
Controller Port Type the Device Controller Port Number here. For HTTP manageable devices, this will most likely be port 80. You can map SNMP to port 161, or another application to its port.

Protocol Select the Protocol Type from the drop-down list box. The values of the drop down are ***TCP*** and ***UDP.***

Connection Select the Connection of the Device from the drop down list box. The values of the drop down are ***Wired*** and ***Wireless***.

2. SYSTEM LOGGING CONFIGURATION

This menu allows the user to configure the syslog settings of the Controller 3000.



Screen 17 System Logging Configuration

System Logging Configuration

This section has two radio buttons, **Enable** and **Disable**. Select either **Enable** to enable the Syslog function or **Disable** to disable the same.

Server Location

If Syslog on LAN Server is checked then type the **LAN IP Address** of the server.

If Syslog on WAN Server is checked then type the **WAN IP Address** of the Syslog Server.

View Syslog is a button which when clicked will show the details of log messages in a pop-up window if Local Syslog is selected.

Syslog Attribute

System Information Check on the **System Information** check box to enable the System Information function and type number of minutes at which the log included system information is to be sent. This provides general system information such as uptime and Controller IP address.

Wireless Association Information Check the **Wireless Association** Information check box to enable the Wireless Association Information function. This provides information for wireless users logins and logouts. Enter the Interval Time in terms of minutes.

Access Point Information Check on the **Access Point Information** check box to include in the log the details of the current LAN Devices Status.

Logged-in Users Check the **Logged-in Users** check box to enable the Logged-in Users Syslog function. Enter the Interval Time in terms of minutes. This SysLog provides a summary of the usage of logged in users.

System Boot Notice Check on the **System Boot Notice** check box to enable the System Boot Notice function. This will send a SysLog message when the Controller boots.

Subscriber Trace Check the **Subscriber Trace** to enable the Subscriber Trace function. This will provide the logged in and logged out time of the subscriber once the user logs out.

Access Point Alarm When this is checked a log would be sent if one of the LAN Devices detection results is "Fail".

Syslog Level One or all the options can be chosen out of Error, Warning, Information, and Debug.

1. Checking the 'Error' option will automatically check only for Errors in Syslog.
2. Checking the 'Warning' option will automatically check only for Warnings and Errors.
3. Checking the 'Information' option will automatically check only for all Syslog Attributes.
4. Checking the 'Debug' option will display debug messages in the controller. The debug output will generate a large volume of SysLog traffic and should only be used if you are having trouble with the Controller.

3.2.7. ADVANCED

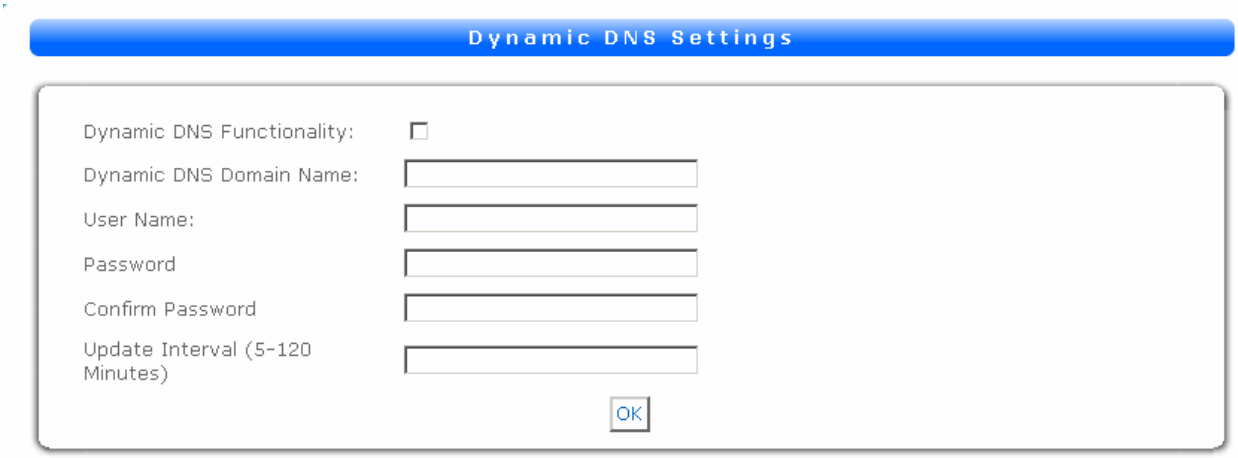
This menu allows you to configure the settings with more advanced features. The Networks menu has four sub-menu tabs,

5. Dynamic DNS
6. GRE Tunnel
7. AuthDirect
8. VLAN Static IPs

Details of the above menus are as follows,

1. DYNAMIC DNS

You can configure the Controller to automatically update domains you have registered at DynDNS.org. Please register with DynDNS.org for instructions on establishing an account and registering devices.



Screen 18 Dynamic DNS Screen Settings

Dynamic DNS Functionality Check this to use dynamic DNS.

Dynamic DNS Domain Name Type the name of the DNS Domain here. It accepts a maximum of 25 characters. This is the domain you registered at DynDNS.org

User Name Type your user name here. It accepts up to 20 characters.

Password	Type your password here. For security purposes, the characters appear in asterisks (*). It accepts up to 20 characters.
Confirm Password	Type the password again here to compare and confirm password. For security purposes, the characters appear in asterisks (*). It accepts up to 20 characters.
Update Interval	This is the interval of updates to the DNS entry. The value typed is calculated in terms of minutes. The Controller will send a message to DynDNS.org at this interval with the current IP address.
Apply	Click **Apply** to implement the settings.

Note: You can also get the current IP address of a Controller receiving DHCP or PPPoE by enabling the system boot SysLog and implementing a Syslog Server in your NOC.

2. GRE TUNNEL

You can configure the Controller to route all authenticated traffic through a Generic Routing Encapsulation (GRE) tunnel. The GRE Tunnel takes all authenticated LAN traffic and transmits it to a remote server over the WAN connection. You can use this feature for content filtering, centralized authentication of multiple sites, or another application you thought of. You will need to configure the receiving end of the GRE tunnel on your server for this to work. Each Controller will need a unique tunnel configuration. This is an advanced feature for expert networking, so it does not really "do" anything other than deliver the traffic to your server. You must build the advanced functionality you want into your server at the other end of the tunnel. This feature is configured under **Advanced – GRE Tunnel**.

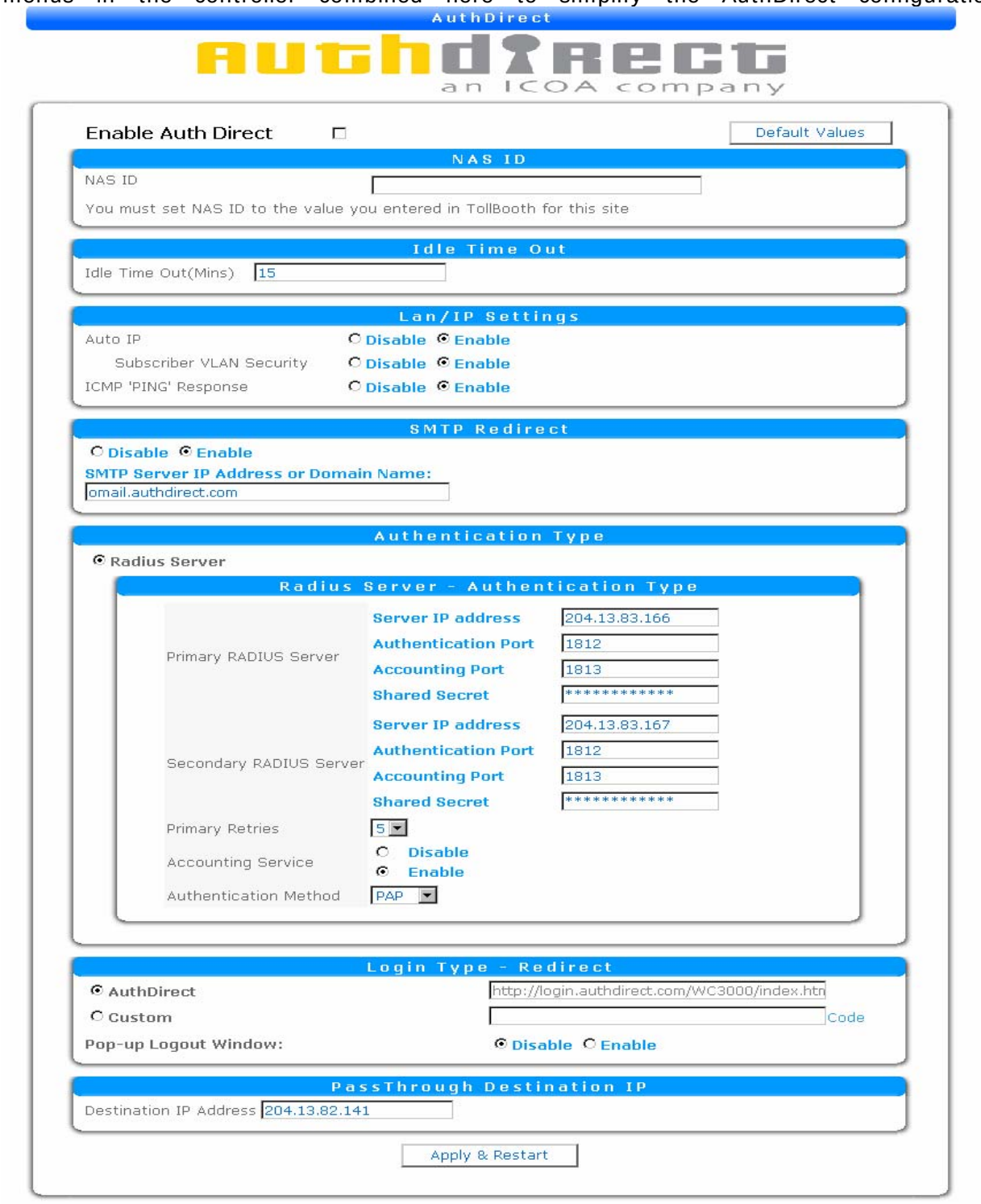
Walled garden and IP pass-through traffic will not be routed through the tunnel, and all normal security, redirection, and authentication features will still be in effect as configured in the Controller.

GRE Tunnel can also be configured on the AuthDirect page. Please contact AuthDirect for details on their content filtering application that uses GRE.

For more information on GRE, see the Linux man pages for "ip tunnel" or the wikipedia.org entry for Generic Routing Encapsulation.

3. AUTHDIRECT

Here the User has an option to configure the Controller as per the settings of AuthDirect. This is similar to the "Express Setup" Menu. This is a combination of different configuration menus in the controller combined here to simplify the AuthDirect configuration.



Screen 19 AuthDirect Configuration

Enable AuthDirect Enabling this would direct the authorized company to give inter access to the subscribers. Values are saved only if "**Enable AuthDirect"** checkbox is selected.

NAS ID NAS ID will be added at the end of AuthDirect URL link for authentication. Please enter the **NAS ID** provided by AuthDirect Here.

Note: You must contact AuthDirect.com for information on using their Billing service.

4. VLAN STATIC IPS

Subscriber Static IP

Subscribers can use one of the provisioned Static IP addresses in their network setup. Prior to authentication, these subscribers are treated like any other subscriber with a proper LAN IP address. After authentication, the subscribers are visible in the controllers WAN side with the Static IP Address configured. They are not NATed by the controller. This feature can be utilized by subscribers using a VPN connection that does not support NAT Traversal, or multiple subscribers using the same VPN server at the same company. Subscribers can get the available static IP addresses automatically from the Static IP address List page. The page contains all the correct IP properties, and the available addresses are displayed automatically.

Subscriber Static IP Select **Enable** to enable the Subscriber Static IP Message page. Static Subscriber IP addresses along with subnet mask, Gateway address and DNS addresses are configured under Networks WAN/LAN if Subscriber Static IP Page is **Enabled.** Select **Disable** if you want subscribers to receive the IP address settings manually, from support for example.

Static Page Title Type the Main Message or Title for the subscriber static IP page in this text box. A maximum of 80 characters are allowed in the text box

Static Page Message Type additional comments to be displayed in the subscriber static IP page.

External Static IP Page HTML Link

You can cut/paste the URL link to the Controller Static IP Address page into your portal page

Preview Click this button to see the current Static IP Address page

Subscriber Static IP Addresses

Type the list of subscriber static IP addresses and the corresponding subnet mask, gateway IP address and DNS IP addresses. A list of 10 static IP addresses can be configured. At least one static IP has to be entered if the Subscriber Static IP option is enabled. The subscriber behind the controller is exposed to the public network by using one of the static IP addresses. A subscriber normally uses these IP addresses if the subscriber is using a VPN connection that does not support NAT Traversal, or if multiple VPN users are accessing the same VPN server at their home company.

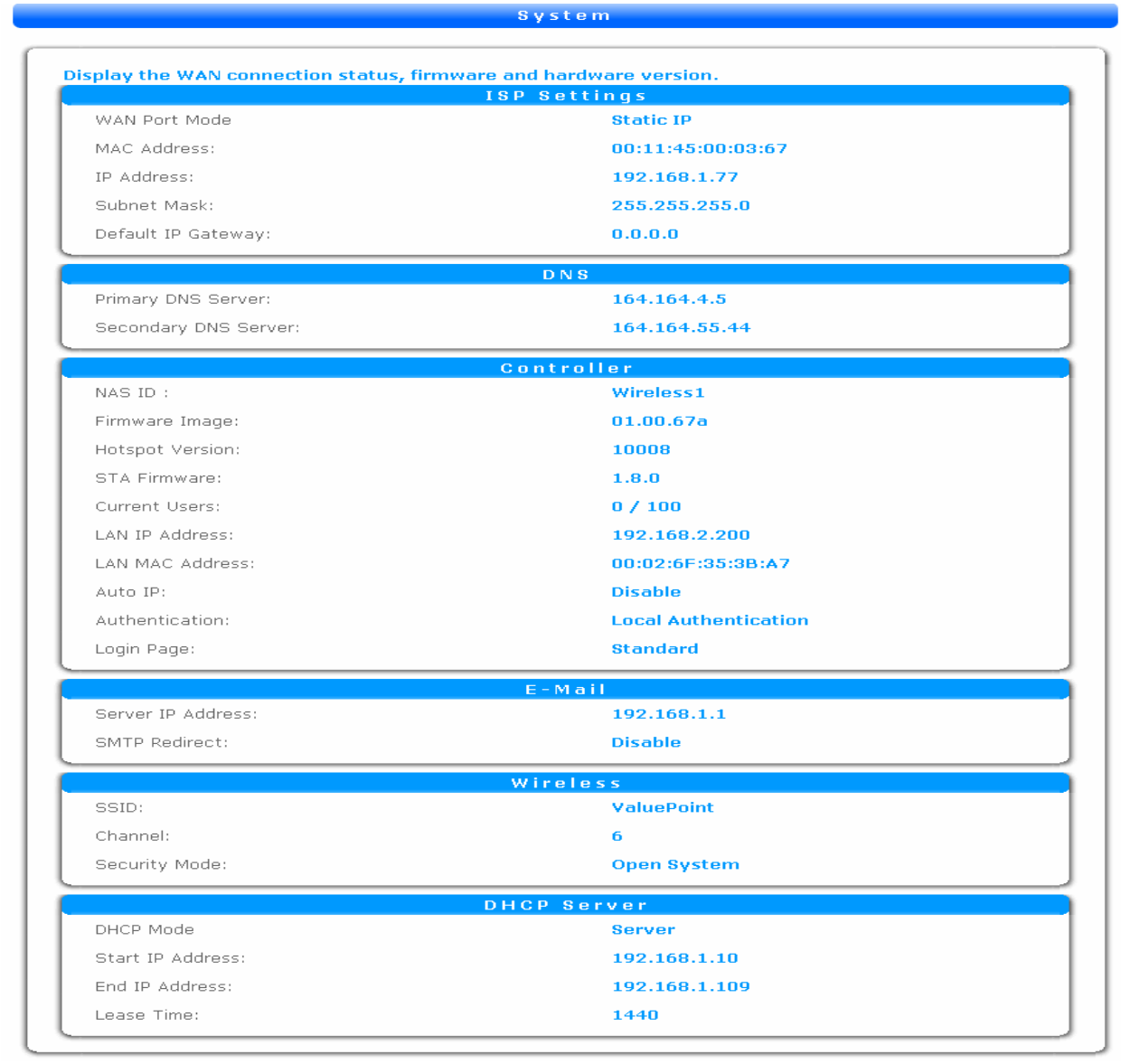
Note: You must obtain valid static public IP addresses from your ISP and provision them into the Controller for VPN and other subscribers to use this feature.

3.2.8. SYSTEM STATUS

This menu tab opens up the sub-menus showing status of the Controller and subscribers.

1. SYSTEM

This menu displays current system information like Host Name, LAN MAC Address, WAN MAC Address, WAN Port Mode, Primary DNS Server, Secondary DNS Server, DHCP Status, Lease Time etc.



Screen 20 System

WAN IP Settings

WAN Port Mode

Here the menu displays the WAN MAC Port Mode.

MAC Address

Here the menu displays the WAN MAC Address of the Controller 3000.

IP Address

Here the menu displays the IP Address of the Controller 3000 WAN Port.

Subnet Mask

Here the menu displays the Subnet Mask of the Controller 3000 WAN Port.

Default IP Gateway

Here the menu displays the Default IP Gateway of the Controller 3000 WAN Port.

DNS

Primary DNS Server

Here the menu displays the IP Address of Primary DNS Server of the Controller 3000.

Secondary DNS Server

Here the menu displays the IP Address of Secondary DNS Server of the Controller 3000.

Controller

NAS ID

Here the menu displays the Host Name of the Controller 3000.

Firmware Image

Here the menu displays the Firmware Version of the Controller 3000.

Hotspot Version

Here the menu displays the HotSpot Configuration Version of the Controller 3000.

STA Firmware (3000 Only)

Here the menu displays the Wireless Version of the Controller 3000.

Current Users

Here the menu displays the Current Users logged into the Controller 3000.

LAN IP Address

Here the menu displays the Controller LAN IP address.

LAN MAC Address

Here the menu displays the LAN MAC Address of the Controller 3000.

Auto IP

This displays the status of Auto IP.

Authentication

The menu displays the authentication type. In the screenshot above, it shows the type as ***Local Authentication***.

Login Page

Here the menu displays the login page type. In the screenshot above it shows it as ***Redirect***.

E-mail

Server IP Address

The E-mail Server IP Addresses.

Wireless(3000 Only)

SSID

Here the menu displays the Controller SSID.

Channel

Here the menu displays the channel number.

Security Mode

Here the menu displays the WiFi security mode.

DHCP Server

DHCP Mode

Here the menu displays the DHCP mode.

Start IP Address

Here the menu displays the DHCP Pool Start IP Address.

End IP Address

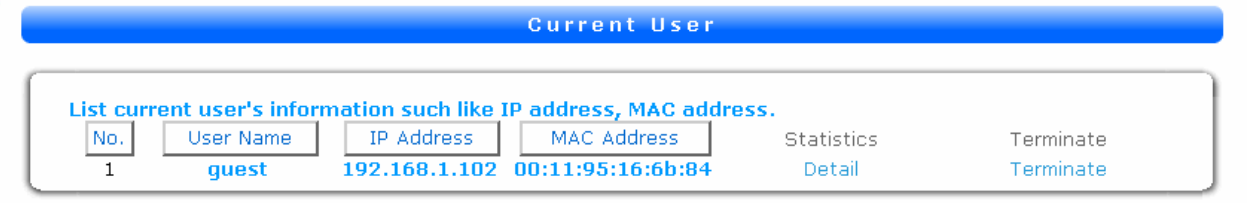
Here the menu displays the DHCP Pool End IP Address.

Lease Time

Here the menu displays the DHCP Lease Time.

2. CURRENT USER

The current user list gives information on users currently authenticated by the Controller.



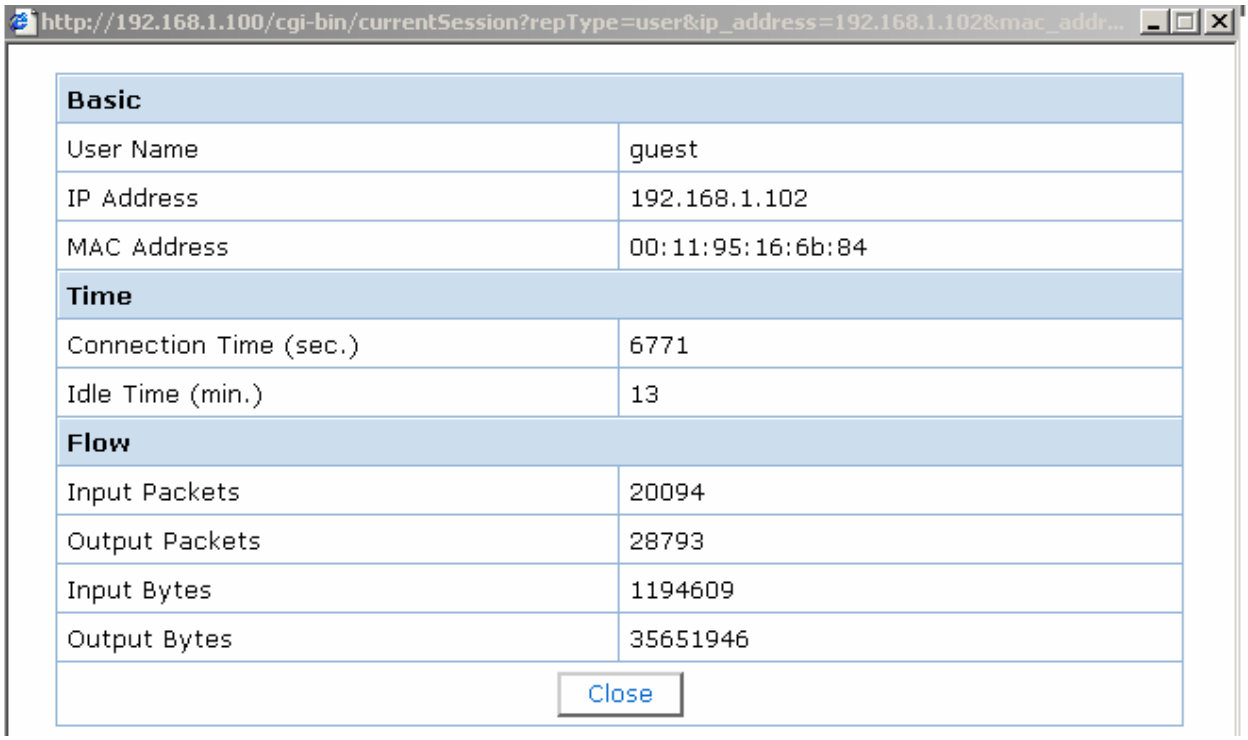
Screen 21 Current User

User Name The user name the subscriber provided when they logged in. This may be blank for some users who did not log in with a username/password.

IP Address Here the menu displays the IP Address of DHCP user.

MAC Address Here the menu displays the MAC Address of DHCP user.

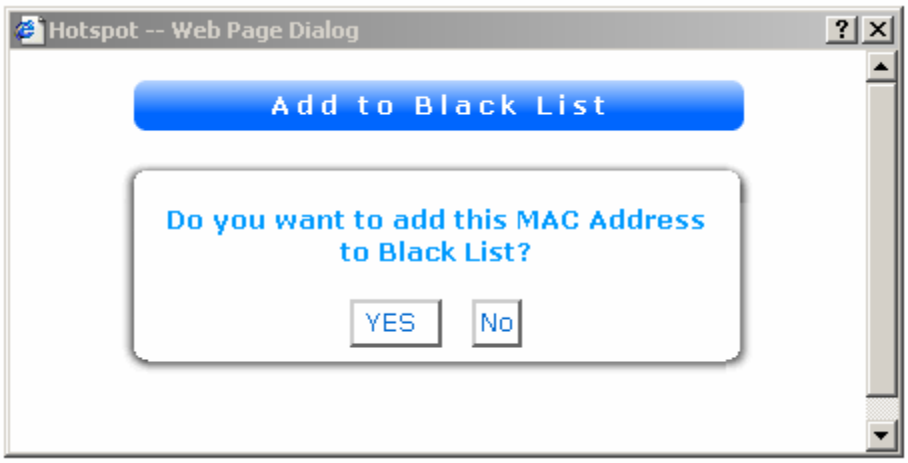
Statistics When you click on ***Detail*** a pop up menu appears giving User status like IP addresses, Mac Address, Connection Time, Idle Time and Packet flow details.



Popup window of Current User Statistics/Detail command

Terminate

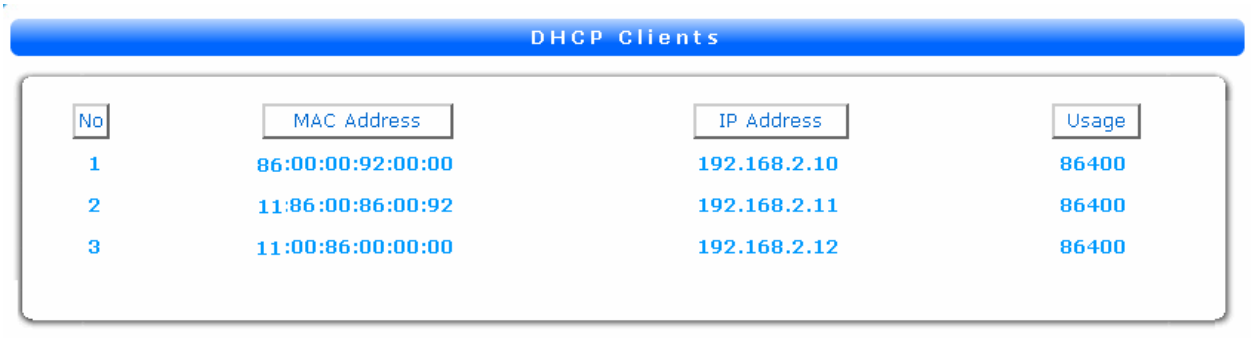
Select this option to log off the user immediately. A pop up menu appears on clicking the 'Terminate' command. This pop-up allows adding the existing client to blacklist entry to deny access next time when '**YES**' button is clicked. It will take a few moments for the access list to be reloaded when you select **YES**.



Popup window of Current User Terminate / Detail command

3. DHCP CLIENT

This menu displays the DHCP user details on LAN. The details displayed are MAC Address and IP Address and usage.



Screen 22 DHCP Clients

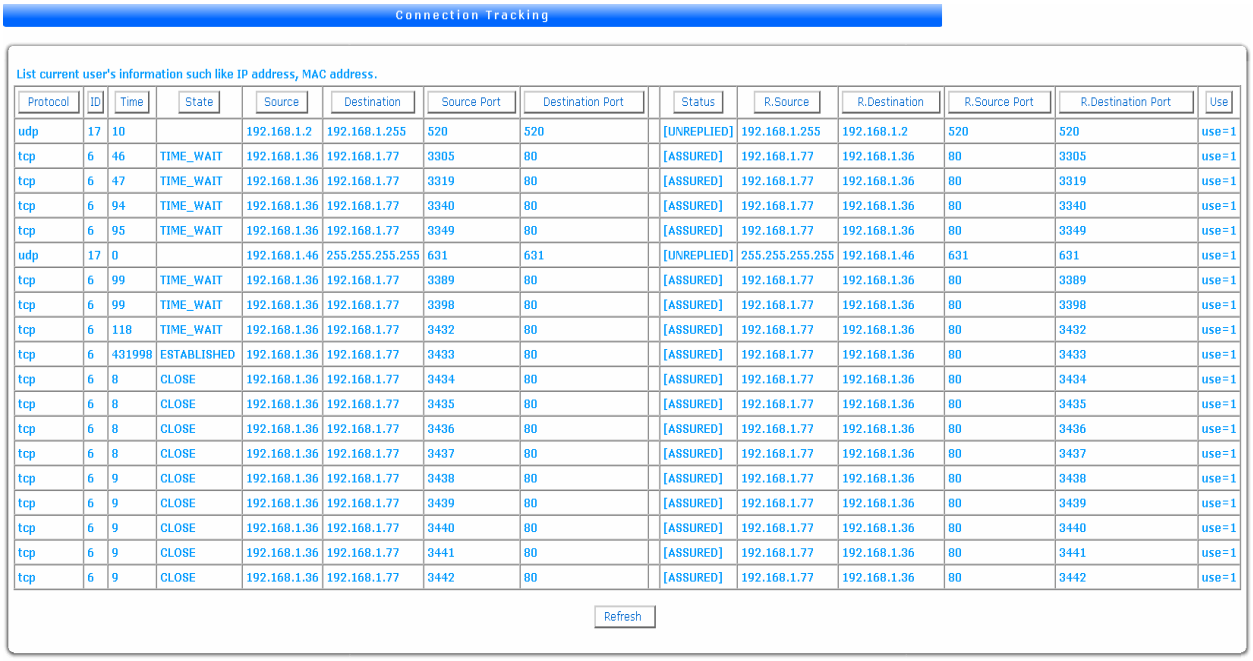
MAC Address The MAC Address of DHCP user.

IP Address The IP Address of DHCP user.

Note: The DHCP Clients table is not an accurate list of subscribers using the service. DHCP Clients only shows PCs that have requested a DHCP address from the Controller in the current session. Subscribers with previous DHCP leases or static IPs will not appear in this table. Logged off subscribers, or random users without accounts, may appear in this table. Use the Current Users table to see logged in users.

4. CONNTRACK

The Connection Tracker allows you to monitor the real time usage status of the Controller 3000 by seeing open and ongoing connections to and from the Controller. This table allows you to monitor subscriber activity and look for unusual behavior caused by worms, viruses, or abusive subscribers.



Connection Tracking

List current user's information such like IP address, MAC address.

Protocol	ID	Time	State	Source	Destination	Source Port	Destination Port	Status	R.Source	R.Destination	R.Source Port	R.Destination Port	Use
udp	17	10		192.168.1.2	192.168.1.255	520	520	[UNREPLIED]	192.168.1.255	192.168.1.2	520	520	use=1
tcp	6	46	TIME_WAIT	192.168.1.36	192.168.1.77	3305	80	[ASSURED]	192.168.1.77	192.168.1.36	80	3305	use=1
tcp	6	47	TIME_WAIT	192.168.1.36	192.168.1.77	3319	80	[ASSURED]	192.168.1.77	192.168.1.36	80	3319	use=1
tcp	6	94	TIME_WAIT	192.168.1.36	192.168.1.77	3340	80	[ASSURED]	192.168.1.77	192.168.1.36	80	3340	use=1
tcp	6	95	TIME_WAIT	192.168.1.36	192.168.1.77	3349	80	[ASSURED]	192.168.1.77	192.168.1.36	80	3349	use=1
udp	17	0		192.168.1.46	255.255.255.255	631	631	[UNREPLIED]	255.255.255.255	192.168.1.46	631	631	use=1
tcp	6	99	TIME_WAIT	192.168.1.36	192.168.1.77	3389	80	[ASSURED]	192.168.1.77	192.168.1.36	80	3389	use=1
tcp	6	99	TIME_WAIT	192.168.1.36	192.168.1.77	3398	80	[ASSURED]	192.168.1.77	192.168.1.36	80	3398	use=1
tcp	6	118	TIME_WAIT	192.168.1.36	192.168.1.77	3432	80	[ASSURED]	192.168.1.77	192.168.1.36	80	3432	use=1
tcp	6	431998	ESTABLISHED	192.168.1.36	192.168.1.77	3433	80	[ASSURED]	192.168.1.77	192.168.1.36	80	3433	use=1
tcp	6	8	CLOSE	192.168.1.36	192.168.1.77	3434	80	[ASSURED]	192.168.1.77	192.168.1.36	80	3434	use=1
tcp	6	8	CLOSE	192.168.1.36	192.168.1.77	3435	80	[ASSURED]	192.168.1.77	192.168.1.36	80	3435	use=1
tcp	6	8	CLOSE	192.168.1.36	192.168.1.77	3436	80	[ASSURED]	192.168.1.77	192.168.1.36	80	3436	use=1
tcp	6	8	CLOSE	192.168.1.36	192.168.1.77	3437	80	[ASSURED]	192.168.1.77	192.168.1.36	80	3437	use=1
tcp	6	9	CLOSE	192.168.1.36	192.168.1.77	3438	80	[ASSURED]	192.168.1.77	192.168.1.36	80	3438	use=1
tcp	6	9	CLOSE	192.168.1.36	192.168.1.77	3439	80	[ASSURED]	192.168.1.77	192.168.1.36	80	3439	use=1
tcp	6	9	CLOSE	192.168.1.36	192.168.1.77	3440	80	[ASSURED]	192.168.1.77	192.168.1.36	80	3440	use=1
tcp	6	9	CLOSE	192.168.1.36	192.168.1.77	3441	80	[ASSURED]	192.168.1.77	192.168.1.36	80	3441	use=1
tcp	6	9	CLOSE	192.168.1.36	192.168.1.77	3442	80	[ASSURED]	192.168.1.77	192.168.1.36	80	3442	use=1

Refresh

Screen 23 ConnTrack

The details found in the connection tracker are,

Protocol The protocol name in this column.

ID The protocol type ID.

Time Time in seconds until entry is cleared from table.

State TCP State of the connection.

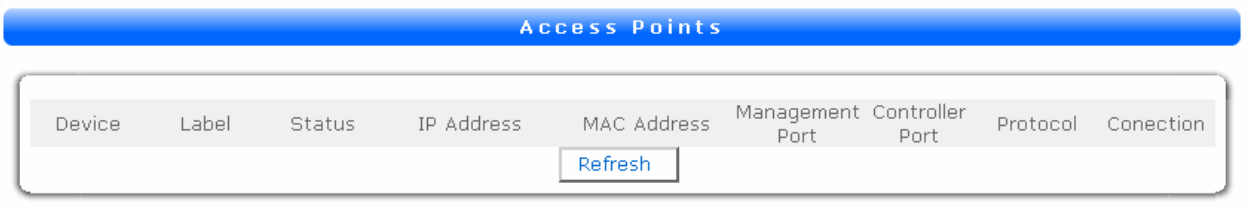
Source Sent source IP address.

Destination	Sent destination IP Address.
Source Port	Sent source port number.
Destination Port	Sent Destination Port number.
Status	Status of the connection. [Unreplied] connections have not received a reply from the destination. [Assured] connections are active connections.
Source	Received source IP address.
Destination	Received destination IP Address.
Source Port	Received source port number.
Destination Port	Received destination port number.
Use	The connection use state. Possible states are: 1. New 2. Established 3. Related (to an established connection) 4. Invalid

Note: You can sort the table by clicking any of these commands. For example, click the command button protocol to sort table based on the protocol details.

5. APs

This menu displays the LAN Devices registered with the Controller 3000. The screen appears as shown here,



Screen 24 Access Points

The field details are,

Device Here the menu displays the LAN device name.

Label Here the menu displays the user defined label.

Status Here the menu displays the status of the device.

IP Address Here the menu displays the Device IP Address.

MAC Address Here the menu displays the device's MAC address.

Management Port Here the menu displays the port number.

Controller Port Here the menu displays the device's server port number.

Protocol Here the menu displays the protocol related to the device.

Connection Here the menu displays the connection.

Refresh This is a command button. When clicked the contents will be refreshed and displayed again with updated details.

6. SYSLOG

This part of the menu displays the system log details for viewing when Local Syslog is enabled. In this example debug messages are enabled.

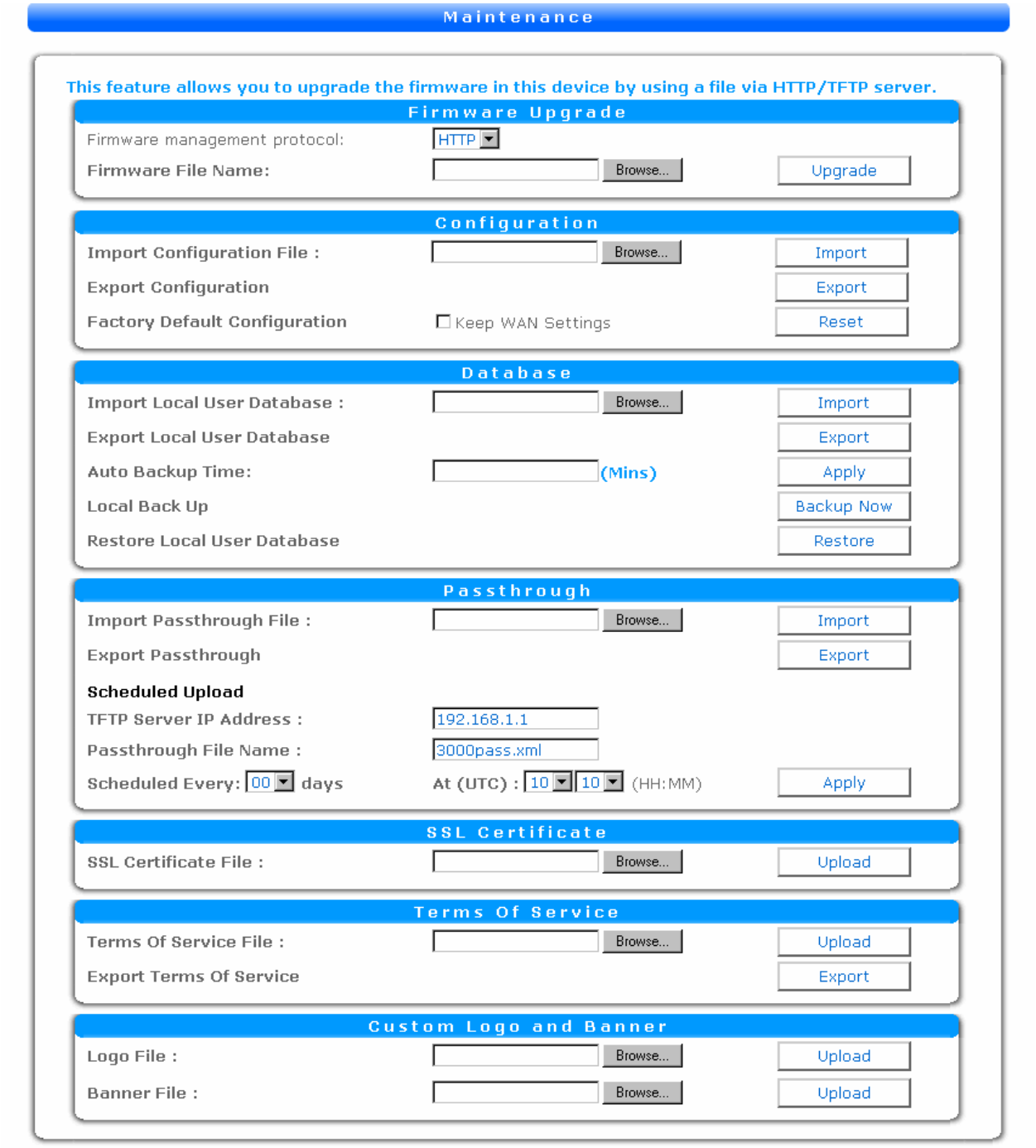
Screen 25 Syslog

The command buttons **First**, **Prev**, **Next** and **Last** will help the user to navigate when there are many pages of log details to be read.

3.2.9. SYSTEM TOOLS

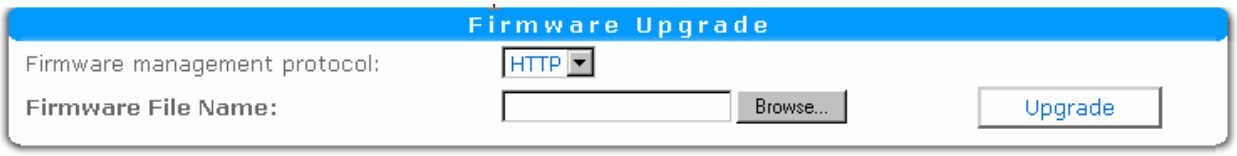
1. MAINTENANCE

This menu allows the user manage the device configuration and to upgrade the firmware in this device by using a file via HTTP or TFTP server. The following screen



Screen 26 Maintenance

Firmware Upgrade



Firmware management Protocol Select the protocol name from the list box. Based on the selection the details on the screen will change.

If the user selects the **TFTP** then the screen will display following details,

Firmware Upgrade

TFTP Server IP Address Enter the IP address of the TFTP server where the Controller can download the firmware image.

TFTP File Name Enter the name of firmware image file available on the TFTP Server.

Upgrade This is a command button. Clicking this will upgrade the selected firmware.

Note: You must have a TFTP server running and configured correctly, and the file name starting with "nfjrom" or "wc3000", for the Controller to download the firmware image. There are many free and commercial TFTP servers, and they all work more or less the same way.

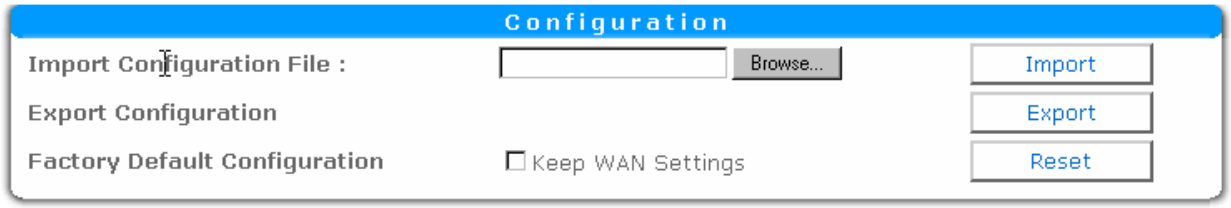
If the user selects the **HTTP** then the screen will display following details,

Firmware Upgrade

Firmware File name Type the name of the file in the text box or click **Browse** and select the file name.

Upgrade Clicking this will upgrade the selected firmware file.

Import Configuration



Import Configuration This section offers the user with an option of restoring the settings of the current device duplicating another devices' configuration information.

Type the file name along with the path name, or simply select the file from the system by clicking the command button labeled as **Browse**. Click ***Import*** to load the selected configuration file.

Export Configuration

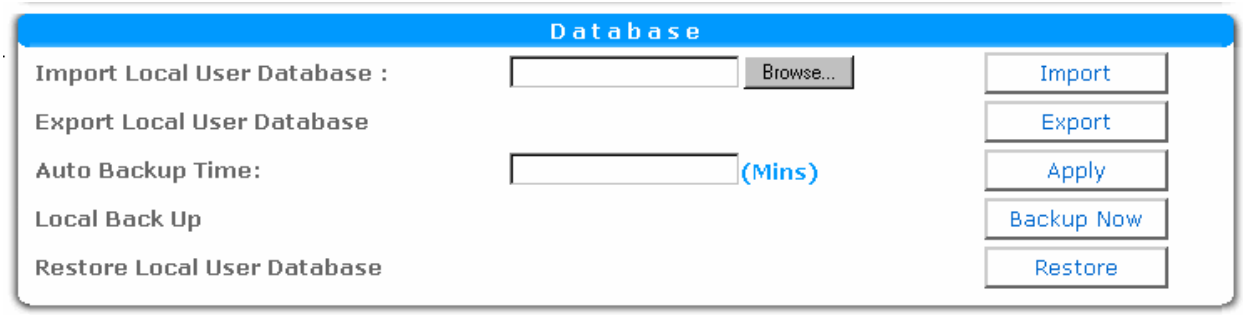
Export Click **Export** to save the current settings to the local system. Right click and select the option of **Save Target As** and save the file to your computer.

Factory Default Configuration

Keep WAN Settings Select this checkbox to keep the current WAN settings when resetting the factory defaults. This will allow you to continue to manage the Controller remotely. Dynamic DNS settings will be preserved as well, in case the Controller is using DHCP.

Reset Click **Reset** to restore the system to the default factory settings. After upgrading, or if the Controller is having problems, it is good to reset the factory defaults.

Database



Import Local User Database This section offers the user with an option of restoring the settings to duplicate the local user database. Type the file name along with the path name or simply select the file from the system by clicking the command button labeled **Browse**. Click ***Import*** to load the user database.

Export Local User Database Click **Export** to save the current user database to the local system. Right click and select the option of Save Target As and save the file to your computer.

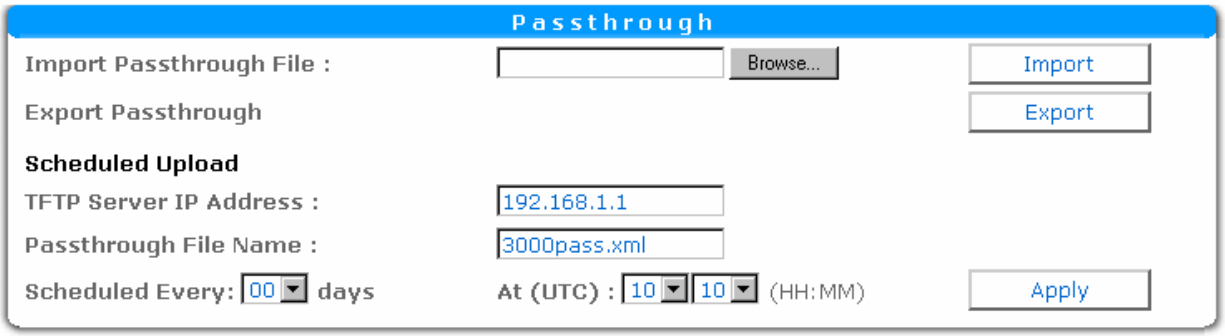
Auto back up time Enter duration in minutes to automatically backup the local user database. The backup is stored in flash on the Controller. Click **Apply** to accept the automatic back up settings.

Local Back Up Click **Backup now** to save the local user database to flash immediately.

Restore Local User Database Click **Restore** to restore the database settings to the copy in flash.

Pass-through

Up to 48 entries for each pass-through value can be entered directly into the GUI. If more entries are required, or entries are to be shared between sites, all of the pass-through entries can be loaded into an XML file and uploaded manually or according to a schedule.



Import pass-through file This has a text box followed by a command button labeled as **Browse**. Type the name of the file in the text box or click **Browse** and select the file name. Clicking the **Import** button will restore the current pass-through entries with the values from the imported file.

Export Pass-through Click **Export** to save the document setting to the local system. Right click and select the option of save 'Target As' and save the file to your computer.

Scheduled Upload

TFTP Server IP Address Enter the TFTP Server IP address to import the pass-through file from the configured TFTP Server address.

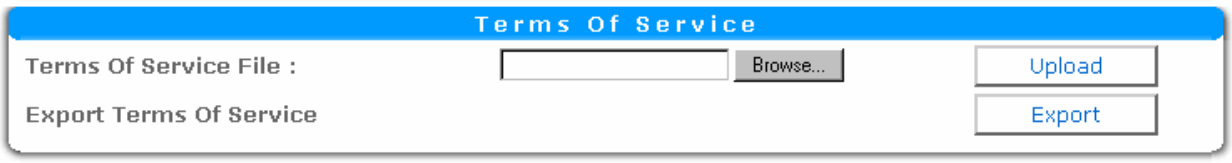
Pass-through File Name Enter the Pass-through file name. By default, it is 3000pass.xml.

Scheduled every This option is configured to import pass-through file automatically from the selected server at the selected time and interval. The first box indicates the frequency of access and the second box indicates the UTC time for the scheduled download.

SSL Certificate

SSL Certificate file Enter the SSL Certificate file name manually in the text box or select the file through the **Browse** button. You must upload a 'self signed' .pem certificate. A self signed certificate can be created by combining your .key and .cert into a single file. Clicking the **Upload** button will upload the certificate to the flash. The uploaded certificate is effective only after the controller reboots. If you upload an incorrect certificate, e.g. not self signed, the Controller will keep rebooting, so you must reset factory defaults by holding the rest button as soon as the system light start to flash.

Terms of Service

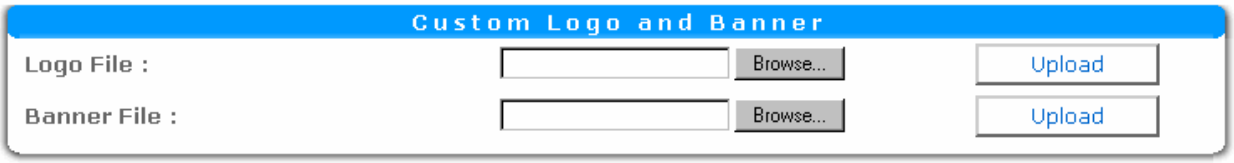


Terms of Service File This has a text box followed by a command button labeled as **Browse**. Type the name of the **Terms of Service** XML file in the text box or click **Browse** and select the file. Special characters if any in the XML file have to be escaped properly as per the XML standards. Use the **Upload** button to upload the file containing Terms of Services or to upload the file after revising the Terms of Service.

Export Terms of Service Click **Export** to save the Terms of Service XML file to the local system. Right click and select the option of save 'Target As' and save the file to your computer

Custom Logo and Banner

You can provide your own custom logo and banner files to brand the internal login pages including Terms of Service and Public Static IP pages.

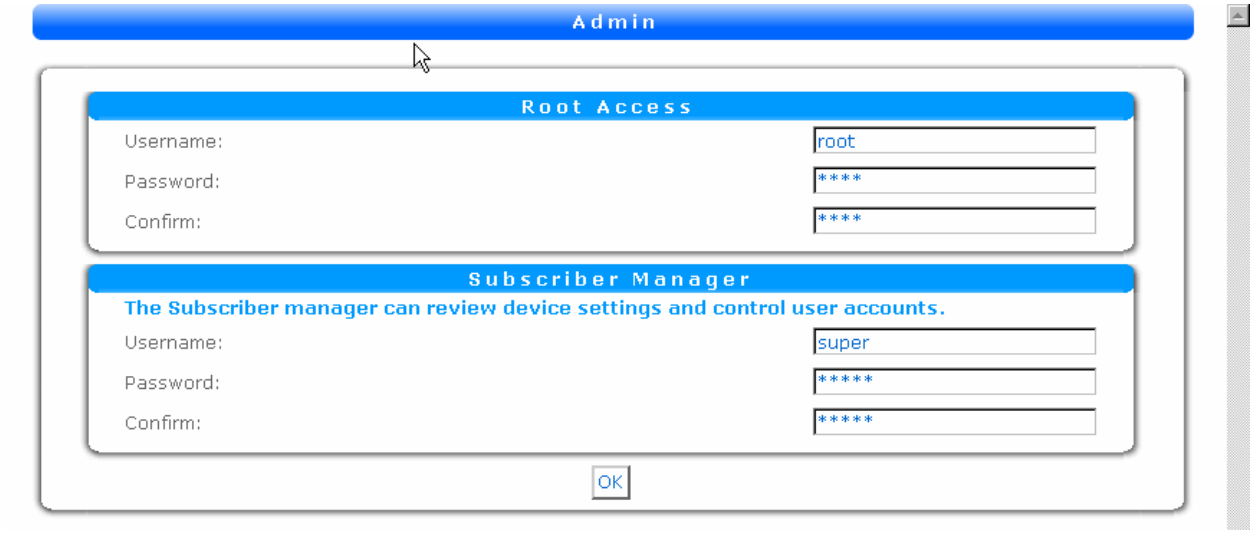


Logo File Any Image File chosen here will be displayed in the Internal/Custom Log in page. Click **Upload** to upload the logo image file.

Banner File Any Image File chosen here will be displayed in the Internal/Custom Log in page. Click **Upload** to upload the banner image file.

Note: The default sizes for the uploaded Banner and Logo files are 519x57 and171x73 respectively. You can upload a smaller or larger image, but the browser will resize it and could distort your image.

2. ADMIN



Screen 27 Admin

Root Access

This section allows creating an administrator and providing the administrator with full control of the system and authority to modify the settings.

Username Type the username here.

Password This is a text box. Type the password here. For the sake of security the characters will appear as asterisks (*) in the box.

Confirm Confirm the password to ensure that password typed in this field and in the **password** are matching.

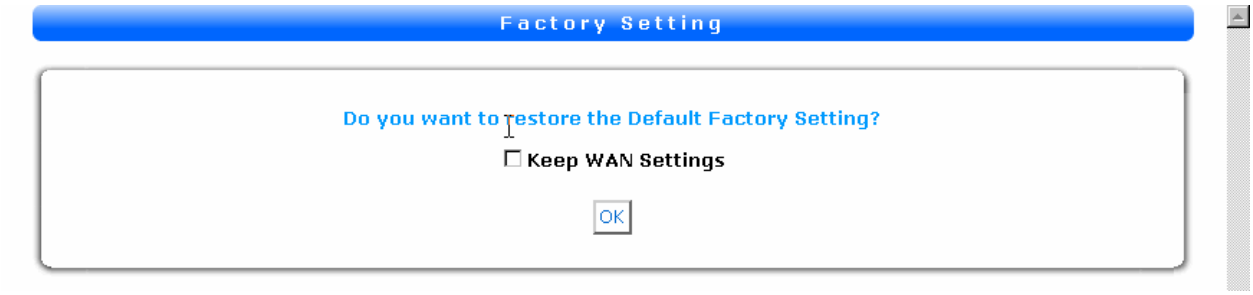
Subscriber Manager

A supervisor account can be created in this section and the supervisor is provided with powers to manage the subscribers and view the system status.

Username	Type the username here.
Password	Type the password here.
Confirm	Confirm the password to ensure that password typed in this field and in the **password** are matching.

3. FACTORY SETTINGS

This submenu allows option for the user to restore the system to its default factory setting. Click **Apply** to restore to the default settings.

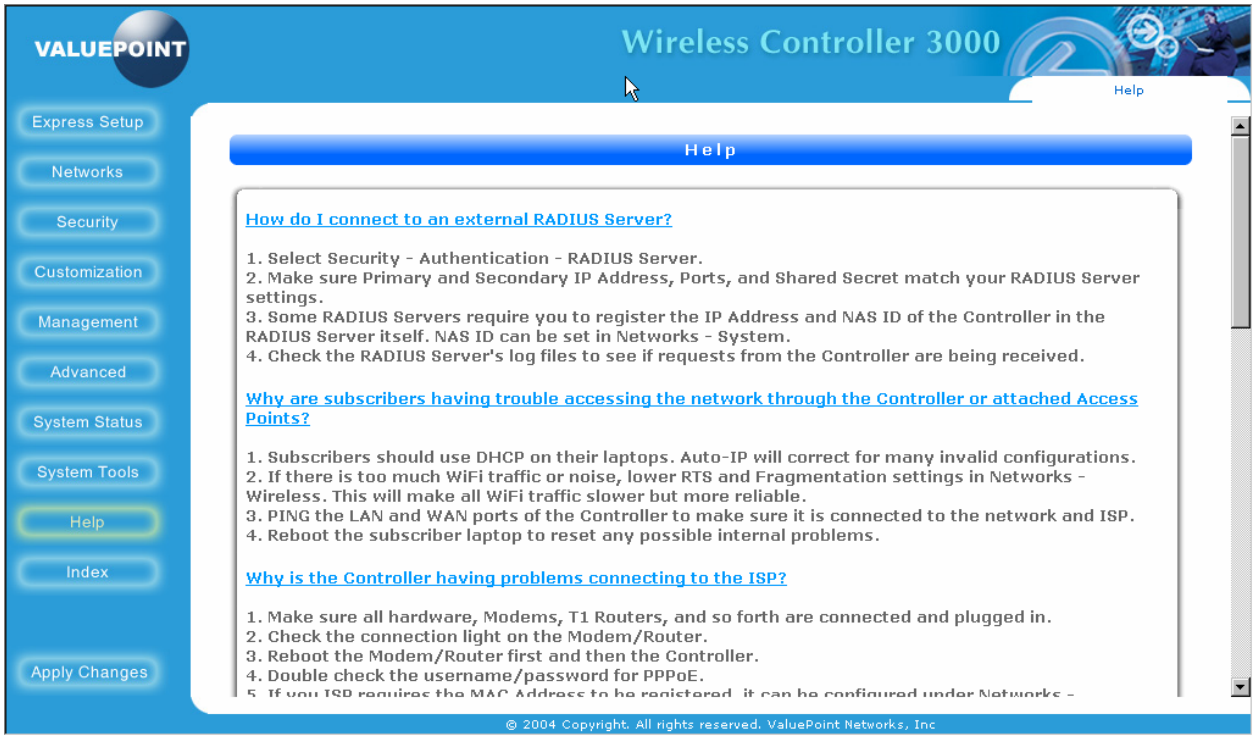


Screen 28 Factory Setting

Keep WAN Settings	Select this checkbox to keep the current WAN settings when resetting the factory defaults. This will allow you to continue to manage the Controller remotely. Dynamic DNS settings will be preserved as well, in case the Controller is using DHCP.
OK	Click **OK** to restore to the default factory setting.

3.2.10. HELP

This menu contains helpful information about the Wireless Controller 3000.

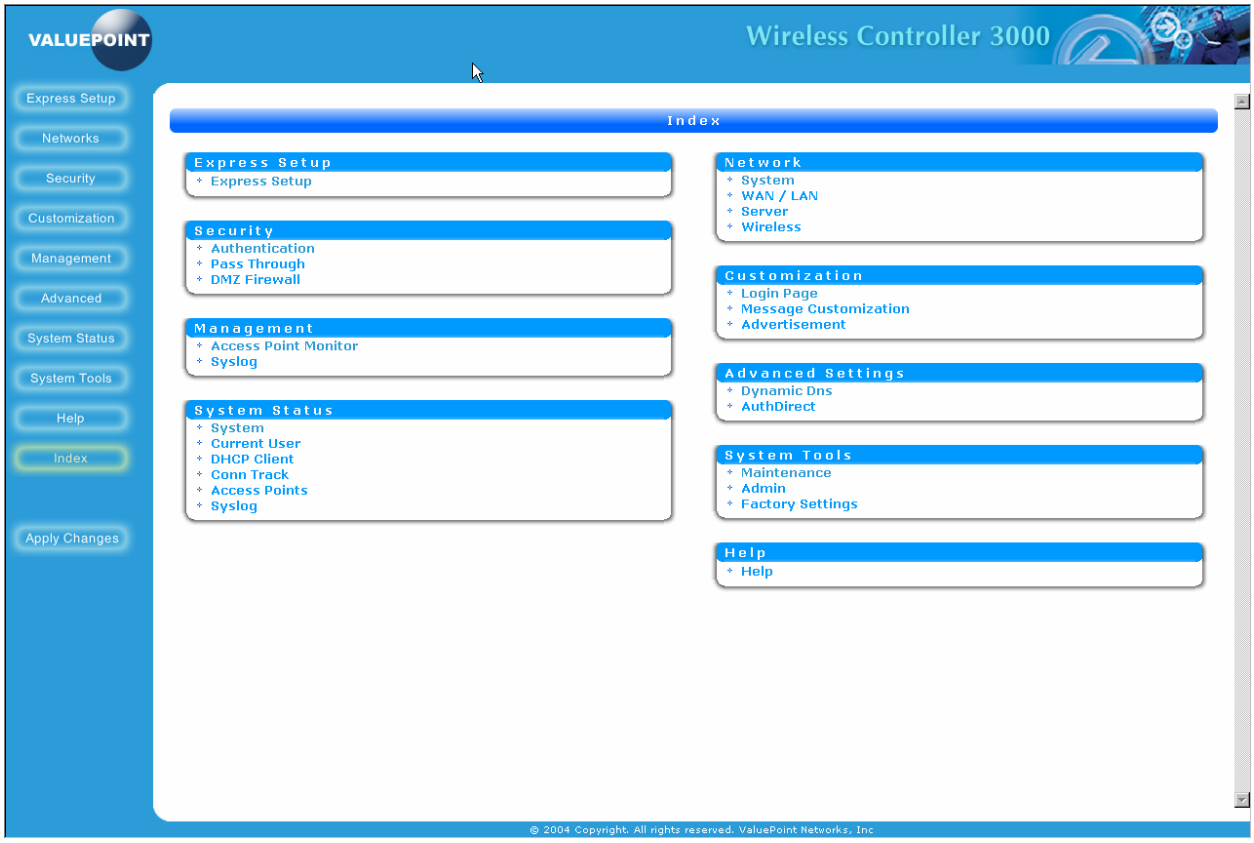


Screen 29 HELP

3.2.11. INDEX

This menu displays all the menus and sub-menus of the Controller that configure the system. Along with the menu, it displays the sub-menus. These sub-menus come with hyperlinks so you can click the tab names and reach the sub-menu directly.

The following screen shows the Index page,



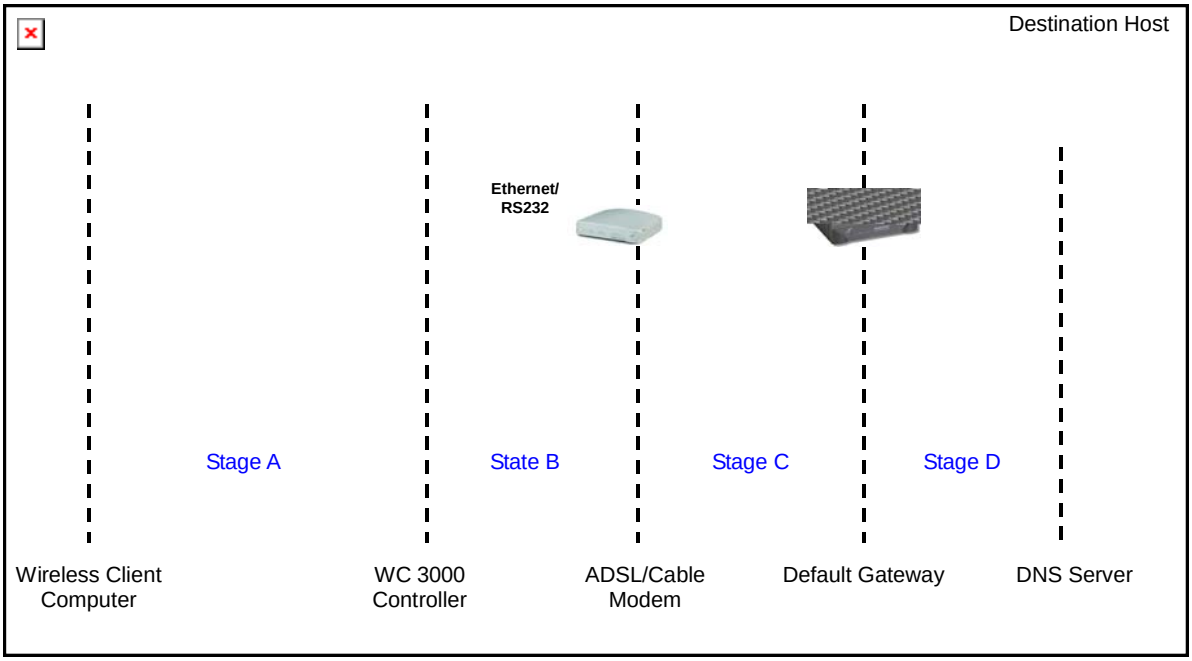
Screen 30 Index

4. TROUBLE SHOOTING

If you have a connectivity problem with the Wireless Controller 3000, check the following first:

- Make sure that the power of the AP is on and the Ethernet cables are connected firmly to the RJ-45 jacks of the AP.
- Make sure that the System LED of the AP is solid to indicate the AP is working and connected to the Internet. A blinking System LED indicates that the Controller has initialized, but the WAN connection is not available. Rebooting the Controller, or both the Controller and the PPPoE/Cable Modem, may restore the WAN connection.
- Make sure the types of the Ethernet cables are correct. There are two types—normal and crossover.

If all Network connections seem normal, use this illustration as a guide to where connection problems can occur:



Communication stages for a client to reach its destination.

For a wireless client computer to communicate with a host on the Internet by the host's domain name (e.g. http://www.valuepointnet.com), it first sends a DNS

request to a DNS server on the Internet. The DNS request travels first to the Controller, and then the Controller relays this request to the default gateway. Finally, this request is forwarded by the default gateway to the DNS server on the Internet. The DNS reply issued by the DNS server is transmitted back to the client computer following a reverse path. When the client computer receives the DNS reply, it knows the IP address of the correspondent host and sends further packets to this IP address.

As illustrated above, the communication path could be broken at several stages. The various OS-provided network diagnostic tools, such as ping.exe or tracert.exe, can be employed to find out TCP/IP-related communication problems.

Note: If two NICs are installed and operating on a client computer, TCP/IP may not work properly due to incorrect entries in the routing table. Use the Windows Device Manager to disable unnecessary NICs. The most common configuration that causes this problem is when the Ethernet and WiFi LAN Cards are both enabled on a laptop at the same time.

4.1. WIFI PROBLEMS (WC-3000 ONLY)

Start by determining if the client is associated with the Controller or a connected Access Point.

- The wireless client computer cannot associate with the Controller/AP.
  - Check the operating mode of the WLAN NIC on the Client.
    - Check that SSID setting of the WLAN NIC and of the Controller/AP match.
  - Is the WEP functionality of the client or Controller/AP enabled?
    - Make appropriate WEP settings of the client computer to match those of the Controller/AP.
  - Is the client within range for wireless communication?
    - Check the signal strength and link quality sensed by the WLAN NIC.
    - Consider using a stronger antenna, amplifier, or additional Access Points.
  - Is the client configured for 802.1x
    - Controller/AP and 802.1x Server settings must match

        - Client must have an 802.1x client and have matching certificate, username/password, or both to connect using 802.1x.

- Associated client experiences poor performance
    - WiFi clients with marginal signal quality may experience slow connections or periodic service outages.
    - When using authentication, unauthenticated client performance is slower than authenticated clients. This may cause pass-through or login pages to load slowly.

4.2. TCP/IP SETTINGS PROBLEMS

If the client is associated, check for client TCP/IP problems

- The Controller does not respond to ping from the client computer.
    - Disable any unused NICs on the client computer.
    - Is Wireless Client or Layer-two isolation enabled on the Controller, or an intervening AP?
        - Disable Isolation features to access local APs or other hardware on the LAN.
    - Check whether the IP address of the client computer and the IP address of the AP are in the same IP sub-net.
        - Turn on Auto-IP to allow clients with invalid static IP Addresses to connect.
        - Enable DHCP on the Controller and client.
- The DNS server(s) do not respond to ping from the client computer.
    - Verify that the Controller WAN port is connected to the ISP by checking the System LED, or checking the Status page in the Controller Web GUI.
    - Verify that the client is authenticated by the Controller, or that the client has opened a HTTP Session (using their web browser) if using No Authentication.

4.3. OTHER PROBLEMS

- The Controller has been set to obtain an IP address automatically by DHCP. How can I know its acquired IP address so that I can manage it using a Web browser?
  - Configure a Dynamic DNS address. You will need to set up an account on DynDNS.org. Please contact DynDNS.org for information and terms of their Dynamic DNS service.
  - If you have access to the DHCP Server, check its client list for the address assigned to the Controller.
  - Reset the Controller to Factory Default, which will restore the default address.
- The Controller stops working and does not respond.
  - Press the Reset button on the Controller.
  - Reset the Controller to Factory Default settings.
  - Unplug the power connector from the power jack, and then re-plug the connector to restart the Controller.
  - Contact our technical support representatives to report this problem, so that any bugs can be solved in future firmware versions.
- If the Controller still does not work after restarting, there may be a hardware component failure in the Controller.
  - Contact our technical support representatives for repair.
- The Controller is working, but I have trouble accessing the Web Management interface.
  - Your browser may have a bad HTML page in the cache. Hold down CTRL and click 'Refresh' button on the browser to force the page to load.
  - Delete the contents of the web cache under Tools – Internet Options – Temporary Internet Files – Delete Files.

- "Repair" the network connection in Windows by right clicking on the connection under Network Neighborhood – Properties and selecting "repair"

5. APPENDICES

5.1. APPENDIX A: SYSLOG MESSAGES

These are some of the more useful information and alarm Syslog messages that can be configured. Please note that "debug" Syslog messages are not included. Any of a vast variety of hardware, application, watchdog, kernel, or other messages can appear when "debug" is selected. **Bold Text** below indicates literal strings you can search for, the other text indicated variables.

System Information – Type: Information (scheduled)

(**ID**: NAS ID) (**System Uptime**: 0 days 00h:04m:00s)
(**WAN**: IPAddr, TxOK, RxOK, TxError, RxError)
(**LAN**: IPAddr, TxOK, RxOK, TxError, RxError)
(**Wireless**: TxOK, RxOK, TxError, RxError)

Wireless Association Information – Type: Information (scheduled)

(**ID**:NAS ID) (**Wireless Association Information**: Number of associated users)

For each user: (**ID**:NAS ID) (**WA**#> MAC address, signal strength, signal quality, connection speed)

Example: (**ID**:NAS ID) (**WA1** . . .)
(**ID**:NAS ID) (**WA2**. . .)
etc.

Logged in Users – Type: Information (scheduled)

(**ID**:NAS ID) (**Logged-in Users**: Number of logged-in users)

For each user: (**ID**:NAS ID) (**User#>** username, user IP, user MAC, interface, login time, RxData, TxData);

Example: (**ID**:NAS ID) (**User1>** . . .)
(**ID**:NAS ID) (**User2>** . . .)
etc.

Subscriber Trace – Type: Warning (sent on subscriber logout)

(**ID**:NAS ID) (**Subscriber Trace**: username, user IP, user MAC, interface, login time, logout time, RxData, TxData)

Lan Devices Info – Information (scheduled)

(**ID**:NAS ID) (**Access Point Monitor**: Number of devices)

For each device: (**ID**:NAS ID) (**Device#>** device label, controller port, device IP, server port, MAC Addr,, tcp/udp, interface, OK/FAIL);

Example: (**ID**:NAS ID) (**device1>** . . .)
(**ID**:NAS ID) (**device2>** . . .)
etc.

Lan Devices Warning – Error (sent on detected FAIL)

(**ID**:NAS ID) (**Access Point Alarm**: device label,**FAIL**)

System Boot Notice – Warning (sent when system boot up is complete)

(**ID**:NAS ID) (**System Boot Notice**, NAS ID, WAN IP Address)

5.2. APPENDIX B: RADIUS ACCOUNTING ATTRIBUTES

User-Name
NAS-IP-Address
NAS-Identifier
Acct-Session-ID
Class-ID (Up to 4 per session)
Calling-Station-ID
Called-Station-ID
Framed-IP
NAS-Port-Type
Acct-Session-Time
Acct-Terminate-Cause
Acct-Output-Packets
Acct-Input-Packets
Acct-Output-Octets
Acct-Input-Octets
Port-Limit (Used for Per-user bandwidth Control)

We send "accounting on" when the Controller boots and an "accounting off" for a normal reboot. It is best practice to clear all current sessions registered to the NAS on receiving “accounting on” or “accounting off”. We do not currently send interim updates.

5.3. APPENDIX C: REGULATORY COMPLIANCE

FCC Regulatory Statement

Part 15-Class B compliant device

This device complies with Part 15 of the FCC Rules. Operation is subject to the following conditions:
1. This device may not cause harmful interference, and

2. This device must accept any interference received, including that which may cause undesired operation.

This equipment has been test and found to comply with the limits for a computing device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. The equipment and the receiver should be connected the outlets on separate circuits.
4. Consult the dealer or an experienced radio/television technician for help.

Changes or modification not expressly approved be the party responsible for compliance could void the user's authority to operate the equipment.

6. LIMITED WARRANTY

Controller 3000

What the warranty covers:
We warrant its products to be free from defects in material and workmanship during the warranty period. If a product proves to be defective in material or workmanship during the warranty period, we will at its sole option repair or replace the product with a like product with a like product. Replacement product or parts may include remanufactured or refurbished parts or components.

How long the warranty is effective:
The Controller 3000 is warranted for one year for all parts and one year for all labor from the date of the first consumer purchase.

Who the warranty protects:
This warranty is valid only for the first consumer purchaser.

What the warranty does not cover:
1. Any product, on which the serial number has been defaced, modified or removed.
2. Damage, deterioration or malfunction resulting from:
a. Accident, misuse, neglect, fire, water, lightning, or other acts of nature, unauthorized product modification, or failure to follow instructions supplied with the product.
b. Repair or attempted repair by anyone not authorized by us.
c. Any damage of the product due to shipment.
d. Removal or installation of the product.
e. Causes external to the product, such as electric power fluctuations or failure.
f. Use of supplies or parts not meeting our specifications.
g. Normal wears and tear.
h. Any other cause that does not relate to a product defect.
3. Removal, installation, and set-up service charges.

How to get service:
1. For information about receiving service under warranty, contact our Customer Support.
2. To obtain warranted service, you will be required to provide (a) the original dated sales slip, (b) your name, (c) your address (d) a description of the problem and (e) the serial number of the product.
3. Take or ship the product prepaid in the original container to your dealer, and our service center.
4. For additional information, contact your dealer or our Customer Service Center.

Limitation of implied warranties:
THERE ARE NO WARRANTIES, EXPRESSED OR IMPLIED, WHICH EXTEND BEYOND THE DESCRIPTION CONTAINED HEREIN INCLUDING THE IMPLIED WARRANTY OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Exclusion of damages:
Our LIABILITY IS LIMITED TO THE COST OF REPAIR OR REPLACEMENT OF THE PRODUCT. We SHALL NOT BE LIABLE FOR:
1. DAMAGE TO OTHER PROPERTY CAUSED BY ANY DEFECTS IN THE PRODUCT, DAMAGES BASED UPON INCONVENCE, LOSS OF USE OF THE PRODUCT, LOSS OF TIME, LOSS OF PROFITS, LOSS OF BUSINESS OPPORTUNITY, LOSS OF GOODWILL, INTERFERENCE WITH BUSINESS RELATIONSHIPS, OR OTHER COMMERCIAL LOSS, EVEN IF ADVISED OF THE POSSIBLITY OF SUCH DAMAGES.
2. ANY OTHER DAMAGES, WHETHER INCIDENTAL, CONSEQUENTIAL OR OTHERWISE.
3. ANY CLAIM AGAINST THE CUSOMER BY ANY OTHER PARTY.